

FILED

2010 JUN -7 PM 12:33
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

1 I. Neel Chatterjee (SBN 173985)
nchatterjee@orrick.com
2 Fabio E. Marino (SBN 183825)
fmarino@orrick.com
3 Qudus B. Olaniran (SBN 267838)
olaniran@orrick.com
4 ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
5 Menlo Park, CA 94025
Telephone: (650) 614-7400
6 Facsimile: (650) 614-7401

7 Robert W. Dickerson (SBN 89367)
rdickerson@orrick.com
8 Benjamin J. Hofileña (SBN 227117)
bhofileña@orrick.com
9 Alyssa M. Caridis (SBN 260103)
acaridis@orrick.com
10 ORRICK, HERRINGTON & SUTCLIFFE LLP
777 South Figueroa Street, Suite 3200
11 Los Angeles, CA 90017
Telephone: 213-629-2020
12 Facsimile: 213-612-2499

13 Attorneys for Defendant and Counterclaimant
14 IBahn CORPORATION

15 IN THE UNITED STATES DISTRICT COURT
16 FOR THE CENTRAL DISTRICT OF CALIFORNIA
17 WESTERN DIVISION

18 NOMADIX, INC.,
19 Plaintiff,
20 v.

21 HEWLETT-PACKARD COMPANY,
WAYPORT, INC., IBahn
22 CORPORATION, GUEST-TEK
INTERACTIVE ENTERTAINMENT
23 LTD., GUEST-TEK INTERACTIVE
ENTERTAINMENT INC., LODGENET
24 INTERACTIVE CORPORATION,
LODGENET STAYONLINE, INC., ON
25 COMMAND CORPORATION,
ARUBA NETWORKS, INC.,
26 SUPERCLICK, INC., SUPERCLICK
NETWORKS, INC.,

27 Defendants.
28

Case No. CV-09-08441-DDP
(VBKx)

**IBAHN CORPORATION'S
COUNTERCLAIMS TO
AMENDED COMPLAINT**

DEMAND FOR JURY TRIAL

Judge: Hon. Dean D. Pregerson

1 IBAHN CORPORATION,
2 Counterclaimant,
3
4 v.
5 NOMADIX, INC.,
6 Counter-defendant.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 Defendant-Counterclaimant iBAHN Corporation ("iBAHN") hereby
2 submits its counterclaims to the Amended Complaint for Patent Infringement of
3 Plaintiff-Counter-defendant Nomadix, Inc. ("Nomadix") as follows:

4 **PARTIES**

5 1. iBAHN Corporation is an entity organized under the laws of the state
6 of Delaware with its principal place of business at 10757 S. River Front Parkway,
7 Suite 300, Salt Lake City, Utah 84095.

8 2. According to the Amended Complaint, Nomadix is a Delaware
9 corporation having its principal place of business at 30851 Agoura Road, Suite 102,
10 Agoura Hills, California 91301.

11 **JURISDICTION AND VENUE**

12 3. Subject to iBAHN's defenses and denials, iBAHN alleges that the
13 Court has jurisdiction over the subject matter of these Counterclaims under, without
14 limitation, 28 U.S.C. §§ 1331, 1367, 1338(a), 2201 and 2202.

15 4. The Court has personal jurisdiction over Plaintiff.

16 5. Venue as to these counterclaims is proper in this district because
17 Plaintiff has submitted to this Court's jurisdiction by the filing of the Amended
18 Complaint in this action.

19 **COUNT ONE - DECLARATORY JUDGMENT OF NON-INFRINGEMENT**

20 6. iBAHN repeats and incorporates by reference its allegations in the
21 foregoing paragraphs.

22 7. Based on the filing by Plaintiff of this suit and iBAHN's defenses, an
23 actual controversy has arisen and now exists between the parties as to whether
24 iBAHN infringes, contributes to the infringement of, or induces infringement of
25 any valid claim of United States Patent Nos. 6,130,892 ("the '892 patent"),
26 7,088,727 ("the '727 patent"), 7,554,995 ("the '995 patent"), 6,636,894 ("the '894
27 patent"), 6,868,399 ("the '399 patent"), or 7,689,716 ("the '716 patent").

28 8. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. §§ 2201

1 *et seq.*, iBAHN requests a declaration from the Court that iBAHN has not infringed
2 any valid claim of the '892, '727, '995, '894, '399, or '716 patents, either directly,
3 contributorily, or by inducement or either literally under the doctrine of equivalents.

4 **COUNT TWO - DECLARATORY JUDGMENT OF INVALIDITY**

5 9. iBAHN repeats and incorporates by reference its allegations in the
6 foregoing paragraphs.

7 10. Based on the filing by Plaintiff of this suit and iBAHN's defenses, an
8 actual controversy has arisen and now exists between the parties as to the validity
9 of each of the claims of the '892, '727, '995, '894, '399, or '716 patents.

10 11. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. §§ 2201
11 *et seq.*, iBAHN requests a declaration from the Court that each of the claims of the
12 '892, '727, '995, '894, '399, or '716 patents are invalid for failure to comply with
13 the provisions of the patent laws, 35 U.S.C. § 100 *et seq.*, including but not limited
14 to one or more of 35 U.S.C. §§ 101, 102, 103, and/or 112.

15 **COUNT THREE – PATENT INFRINGEMENT**

16 12. iBAHN repeats and incorporates by reference its allegations in the
17 foregoing paragraphs.

18 13. United States Patent No. 6,934,754 (“the '754 patent”), entitled
19 “Methods and apparatus for processing network data transmissions,” was duly and
20 legally issued by the United States Patent and Trademark Office on August 23,
21 2005, after full and fair examination. iBAHN is the assignee of all rights, title, and
22 interest in and to the '754 patent and possess all rights of recovery under the '754
23 patent, including the right to sue for infringement and recover past damages. A
24 copy of the '754 patent is attached as Exhibit 1.

25 14. Nomadix sells and distributes, including, upon information and belief,
26 sales and distribution within the Central District of California, gateway devices
27 including but not limited to products sold under the name AG 3100, AG 5000, and
28

1 AG 5500 Metro Bundle.

2 15. Nomadix has infringed, and continues to infringe, the '754 patent by
3 making, using, offering to sell, selling (directly or through intermediaries) within the
4 United States, and/or importing into the United States products covered by one or
5 more claims of the '754 patent, and/or by contributorily infringing one or more claims
6 of the '754 patent, all without the authorization of iBAHN, including but not limited to
7 the products identified in paragraph 21.

8 16. Upon information and belief, Nomadix has been and still is actively
9 inducing one or more third parties to infringe one or more claims of the '754 patent,
10 all without the authorization of iBAHN.

11 17. Nomadix has constructive notice of the '754 patent and of their
12 infringement of the '754 patent.

13 18. As a result of the infringement by Nomadix, iBAHN has suffered, and
14 will continue to suffer, damages. iBAHN is entitled to recover from Nomadix the
15 damages sustained as a result of Nomadix's wrongful acts in an amount subject to
16 proof at trial.

17 19. The infringement by Nomadix of iBAHN's rights under the '754 patent
18 will continue to damage iBAHN, causing irreparable harm for which there is no
19 adequate remedy at law, unless Nomadix is enjoined by this Court.

20 **COUNT FOUR – PATENT INFRINGEMENT**

21 20. iBAHN repeats and incorporates by reference its allegations in the
22 foregoing paragraphs.

23 21. United States Patent No. 6996,073 ("the '073 patent"), entitled
24 "Methods and apparatus for providing high speed connectivity to a hotel
25 environment," was duly and legally issued by the United States Patent and
26 Trademark Office on February 7, 2006, after full and fair examination. iBAHN is
27 the assignee of all rights, title, and interest in and to the '073 patent and possess all
28 rights of recovery under the '073 patent, including the right to sue for infringement

1 and recover past damages. A copy of the '073 patent is attached as Exhibit 2.

2 22. Nomadix has infringed, and continues to infringe, the '073 patent by
3 making, using, offering to sell, selling (directly or through intermediaries) within
4 the United States, and/or importing into the United States products covered by one
5 or more claims of the '073 patent, and/or by contributorily infringing one or more
6 claims of the '073 patent, all without the authorization of iBAHN, including but not
7 limited to the products identified in paragraph 14.

8 23. Upon information and belief, Nomadix has been and still is actively
9 inducing one or more third parties to infringe one or more claims of the '073 patent,
10 all without the authorization of iBAHN.

11 24. Nomadix has constructive notice of the '073 patent and of their
12 infringement of the '073 patent.

13 25. As a result of the infringement by Nomadix, iBAHN has suffered, and
14 will continue to suffer, damages. iBAHN is entitled to recover from Nomadix the
15 damages sustained as a result of Nomadix's wrongful acts in an amount subject to
16 proof at trial.

17 26. The infringement by Nomadix of iBAHN's rights under the '073
18 patent will continue to damage iBAHN, causing irreparable harm for which there is
19 no adequate remedy at law, unless Nomadix is enjoined by this Court.

20 **COUNT FIVE – PATENT INFRINGEMENT**

21 27. iBAHN repeats and incorporates by reference its allegations in the
22 foregoing paragraphs.

23 28. United States Patent No. 7,580,376 ("the '376 patent"), entitled
24 "Methods and apparatus for providing high speed connectivity to a hotel
25 environment," was duly and legally issued by the United States Patent and
26 Trademark Office on August 25, 2009, after full and fair examination. iBAHN is
27 the assignee of all rights, title, and interest in and to the '376 patent and possess all
28 rights of recovery under the '376 patent, including the right to sue for infringement

1 and recover past damages. A copy of the '376 patent is attached as Exhibit 3.

2 29. Nomadix has infringed, and continues to infringe, the '376 patent by
3 making, using, offering to sell, selling (directly or through intermediaries) within
4 the United States, and/or importing into the United States products covered by one
5 or more claims of the '376 patent, and/or by contributorily infringing one or more
6 claims of the '376 patent, all without the authorization of iBAHN, including but not
7 limited to the products identified in paragraph 14.

8 30. Upon information and belief, Nomadix has been and still is actively
9 inducing one or more third parties to infringe one or more claims of the '376 patent,
10 all without the authorization of iBAHN.

11 31. Nomadix has constructive notice of the '376 patent and of their
12 infringement of the '376 patent.

13 32. As a result of the infringement by Nomadix, iBAHN has suffered, and
14 will continue to suffer, damages. iBAHN is entitled to recover from Nomadix the
15 damages sustained as a result of Nomadix's wrongful acts in an amount subject to
16 proof at trial.

17 33. The infringement by Nomadix of iBAHN's rights under the '376
18 patent will continue to damage iBAHN, causing irreparable harm for which there is
19 no adequate remedy at law, unless Nomadix is enjoined by this Court.

20 **EXCEPTIONAL CASE**

21 34. To the extent this is an exceptional case under 35 U.S.C. § 285,
22 iBAHN is entitled to recover from Plaintiff iBAHN's attorneys' fees and costs
23 incurred in connection with this action.

24 **RESERVATION OF RIGHTS**

25 35. iBAHN hereby reserves its right to supplement with additional
26 defenses as discovery proceeds in this matter.

27 **PRAYER**

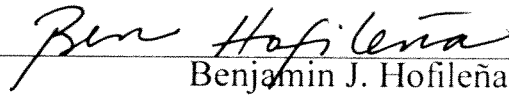
28 WHEREFORE, iBAHN prays for judgment as follows:

- 1 1. A judgment that Nomadix take nothing by its Complaint, and that its
2 Complaint against iBAHN be dismissed with prejudice;
- 3 2. A judgment in favor of iBAHN on all of its Counterclaims;
- 4 3. A declaration that iBAHN has not infringed, either directly or
5 indirectly, any valid and enforceable claim of the '892, '727, '995, '894, '399, or
6 '716 patents;
- 7 4. A declaration that the '892, '727, '995, '894, '399, or '716 patents are
8 invalid and/or unenforceable;
- 9 5. A declaration that Nomadix has infringed, contributed to the
10 infringement of, and/or induced infringement of the '754, '073, and '376 patents;
- 11 6. A declaration that the '754, '073, and '376 patents are valid and
12 enforceable;
- 13 7. A permanent injunction enjoining Nomadix, including its officers,
14 agents, servants, employees, and those persons acting in active concert or in
15 participation with Nomadix, from infringing the '754, '073, and '376 patents;
- 16 8. An accounting of all gains, profits, and advantages derived by
17 Nomadix's infringement of the '754, '073, and '376 patents and an award of
18 damages adequate to compensate iBAHN for Nomadix's direct, contributory,
19 and/or inducement of infringement of the '754, '073, and '376 patents, together
20 with pre-judgment and post-judgment interest;
- 21 9. A declaration that this case is exceptional and an award to iBAHN of
22 its reasonable costs and expenses, including attorneys' fees and expert witness fees;
- 23 10. Such other and further relief as the Court may deem proper.

1 Dated: June 7, 2010

Respectfully submitted,

2 ORRICK, HERRINGTON & SUTCLIFFE LLP

3 
4 Benjamin J. Hofileña

5 I. Neel Chatterjee (SBN 173985)
6 Fabio E. Marino (SBN 183825)
7 Qudus B. Olaniran (SBN 267838)
8 1000 Marsh Road
9 Menlo Park, CA 94025
10 Telephone: (650) 614-7400
11 Facsimile: (650) 614-7401

12 Robert W. Dickerson (SBN 89367)
13 Benjamin J. Hofileña (SBN 227117)
14 Alyssa M. Caridis (SBN 260103)
15 777 South Figueroa Street, Suite 3200
16 Los Angeles, CA 90017
17 Telephone: 213-629-2020
18 Facsimile: 213-612-2499

19 Attorneys for Defendant and Counterclaimant
20 IBAHN CORPORATION

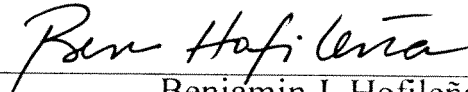
DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Defendant and Counterclaimant iBAHN Corporation hereby demands a trial by jury on all issues so triable.

Dated: June 7, 2010

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP



Benjamin J. Hofileña

I. Neel Chatterjee (SBN 173985)
Fabio E. Marino (SBN 183825)
Qudus B. Olaniran (SBN 267838)
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Robert W. Dickerson (SBN 89367)
Benjamin J. Hofileña (SBN 227117)
Alyssa M. Caridis (SBN 260103)
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017
Telephone: 213-629-2020
Facsimile: 213-612-2499

Attorneys for Defendant and Counterclaimant
IBAHN CORPORATION

EXHIBIT 1

(12) **United States Patent**
West et al.

(10) **Patent No.:** **US 6,934,754 B2**
(45) **Date of Patent:** ***Aug. 23, 2005**

(54) **METHODS AND APPARATUS FOR
PROCESSING NETWORK DATA
TRANSMISSIONS**

(75) Inventors: **William B. West**, Salt Lake City, UT
(US); **Wallace Eric Smith**, Lindon, UT
(US)

(73) Assignee: **iBAHN General Holdings, Inc.**, South
Jordan, UT (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 918 days.

This patent is subject to a terminal dis-
claimer.

(21) Appl. No.: **09/823,088**

(22) Filed: **Mar. 29, 2001**

(65) **Prior Publication Data**

US 2001/0037391 A1 Nov. 1, 2001

Related U.S. Application Data

(60) Provisional application No. 60/194,354, filed on Apr. 3,
2000.

(51) **Int. Cl.**⁷ **G06F 15/173**

(52) **U.S. Cl.** **709/225; 709/220; 709/223;**
709/224; 709/226; 370/401; 370/475

(58) **Field of Search** **709/220, 223–226,**
709/230, 238, 245, 249; 370/401, 475,
351–356, 389, 254

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,790,548 A * 8/1998 Sistanizadeh et al. 370/401

5,793,763 A 8/1998 Mayes et al. 370/389
5,812,819 A * 9/1998 Rodwin et al. 703/23
5,835,725 A * 11/1998 Chiang et al. 709/228
6,052,725 A * 4/2000 McCann et al. 709/223
6,058,431 A * 5/2000 Srisuresh et al. 709/245
6,061,349 A 5/2000 Coile et al. 370/389
6,118,768 A 9/2000 Bhatia et al. 370/254
6,128,657 A 10/2000 Okanoya et al. 709/224
6,393,017 B1 * 5/2002 Galvin et al. 370/352
6,614,774 B1 * 9/2003 Wang 370/338
6,738,382 B1 * 5/2004 West et al. 370/401

FOREIGN PATENT DOCUMENTS

EP 1017208 A2 * 7/2000 H04L/29/12

* cited by examiner

Primary Examiner—Bharat Barot

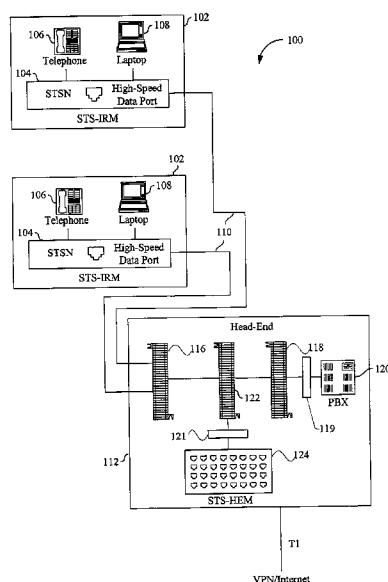
Assistant Examiner—Liang-che Wang

(74) *Attorney, Agent, or Firm*—Beyer Weaver & Thomas
LLP

(57) **ABSTRACT**

Methods and apparatus are described for providing access to
a network via a first one of a plurality of network access
nodes in the network. The network access nodes each have
a network address associated therewith which is unique on
the network, the first network access node having a first
network address associated therewith. The first network
address is associated with a first computer while the first
computer is connected to the first network access node
thereby providing access to the network. Transmissions
associated with the first computer are monitored to deter-
mine address information. The transmissions are then pro-
cessed in response to the address information.

25 Claims, 8 Drawing Sheets



U.S. Patent

Aug. 23, 2005

Sheet 1 of 8

US 6,934,754 B2

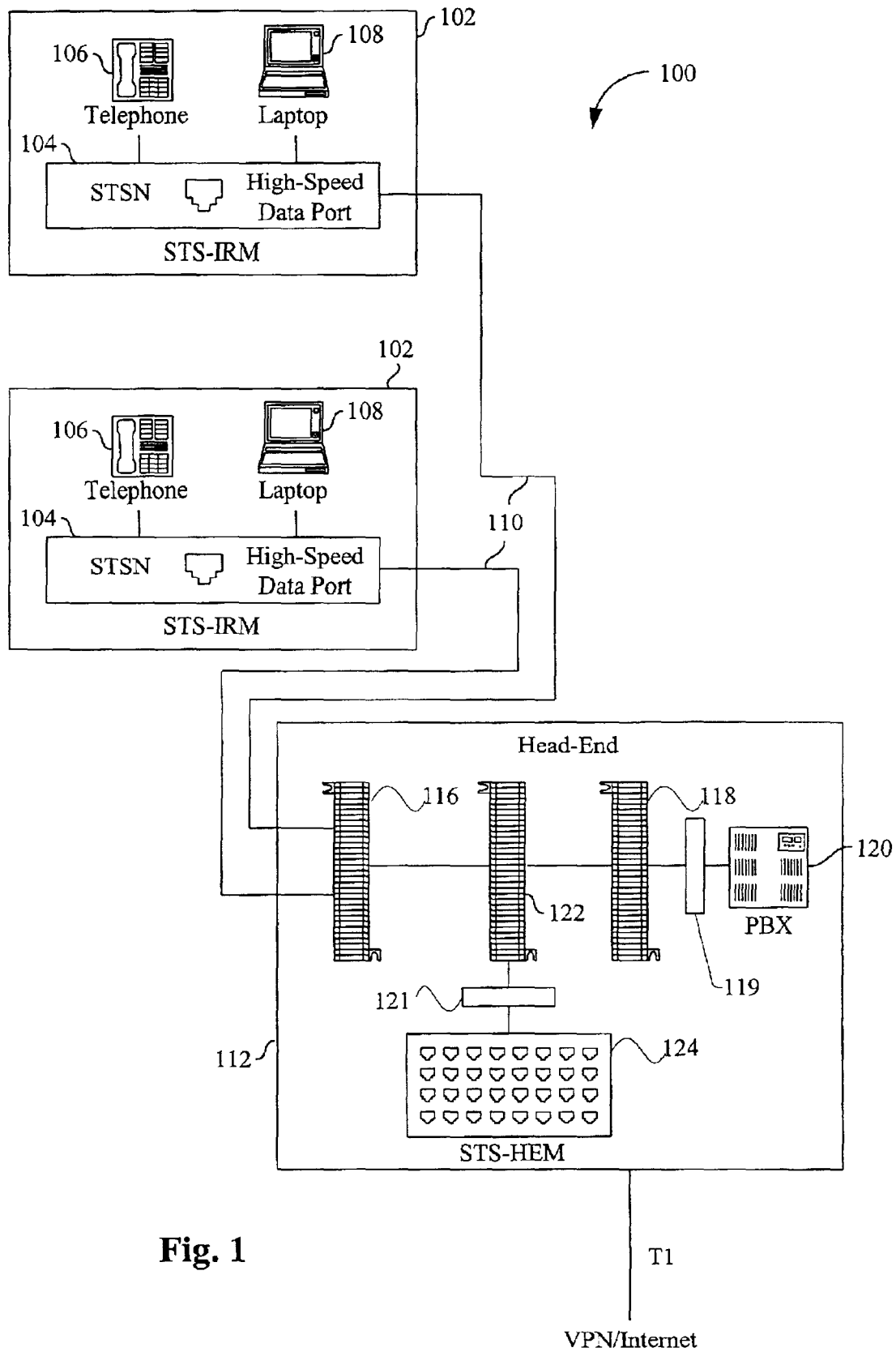


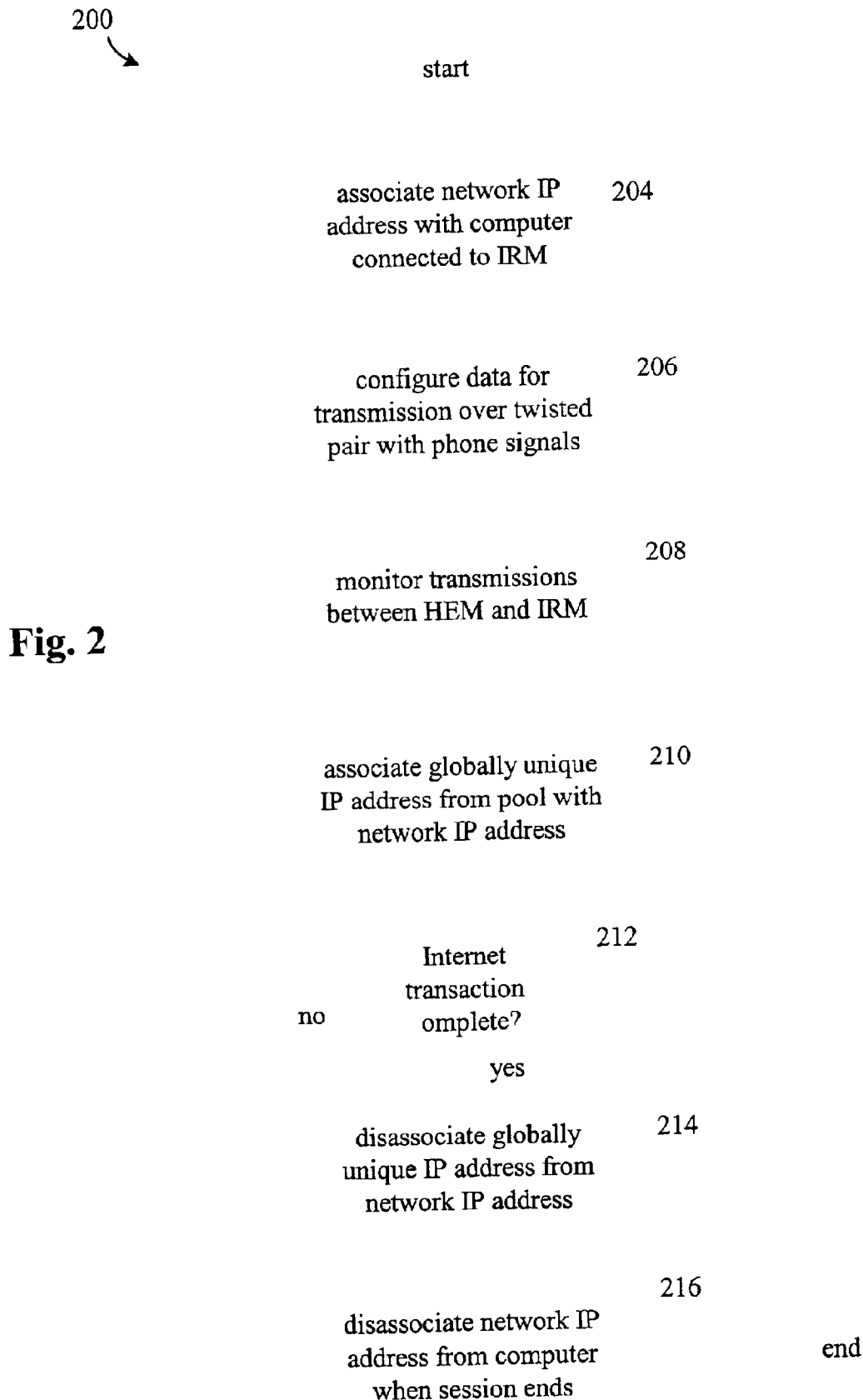
Fig. 1

U.S. Patent

Aug. 23, 2005

Sheet 2 of 8

US 6,934,754 B2



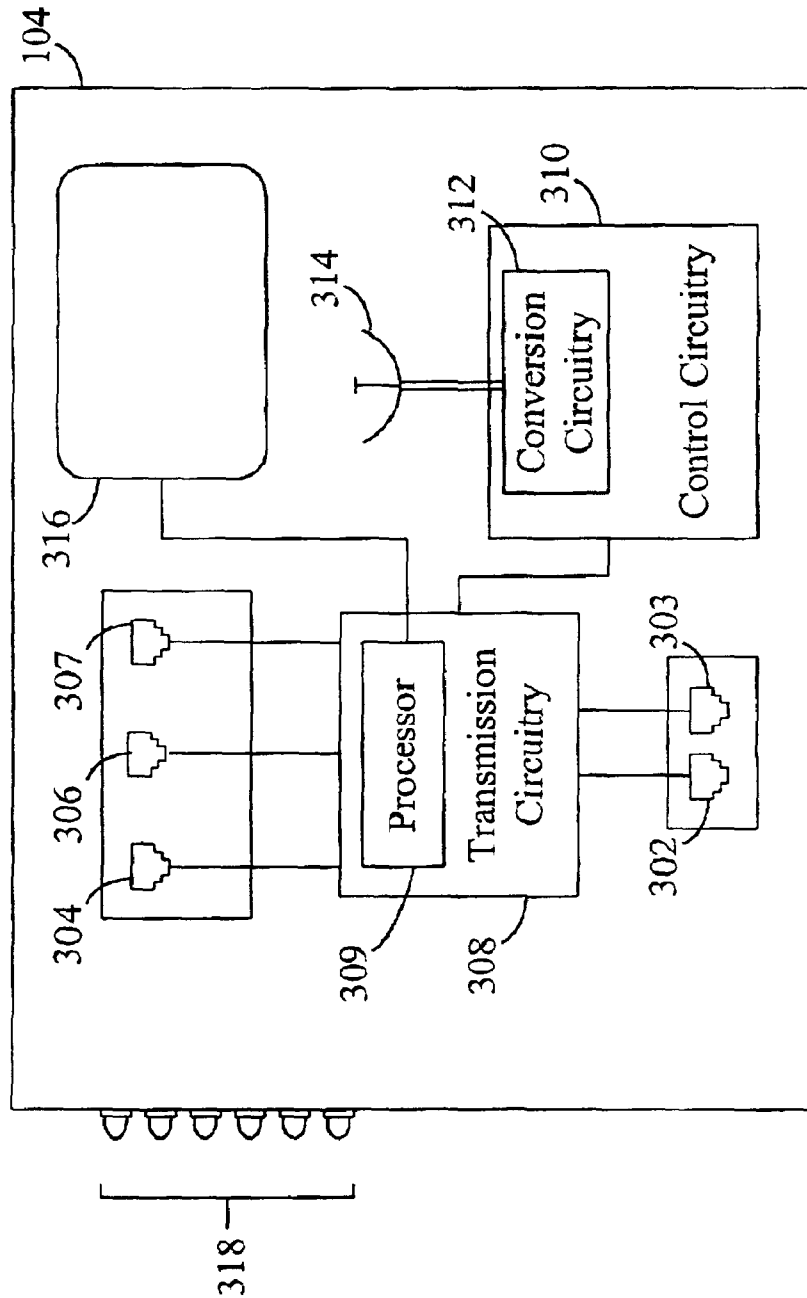


Fig. 3a

U.S. Patent

Aug. 23, 2005

Sheet 4 of 8

US 6,934,754 B2

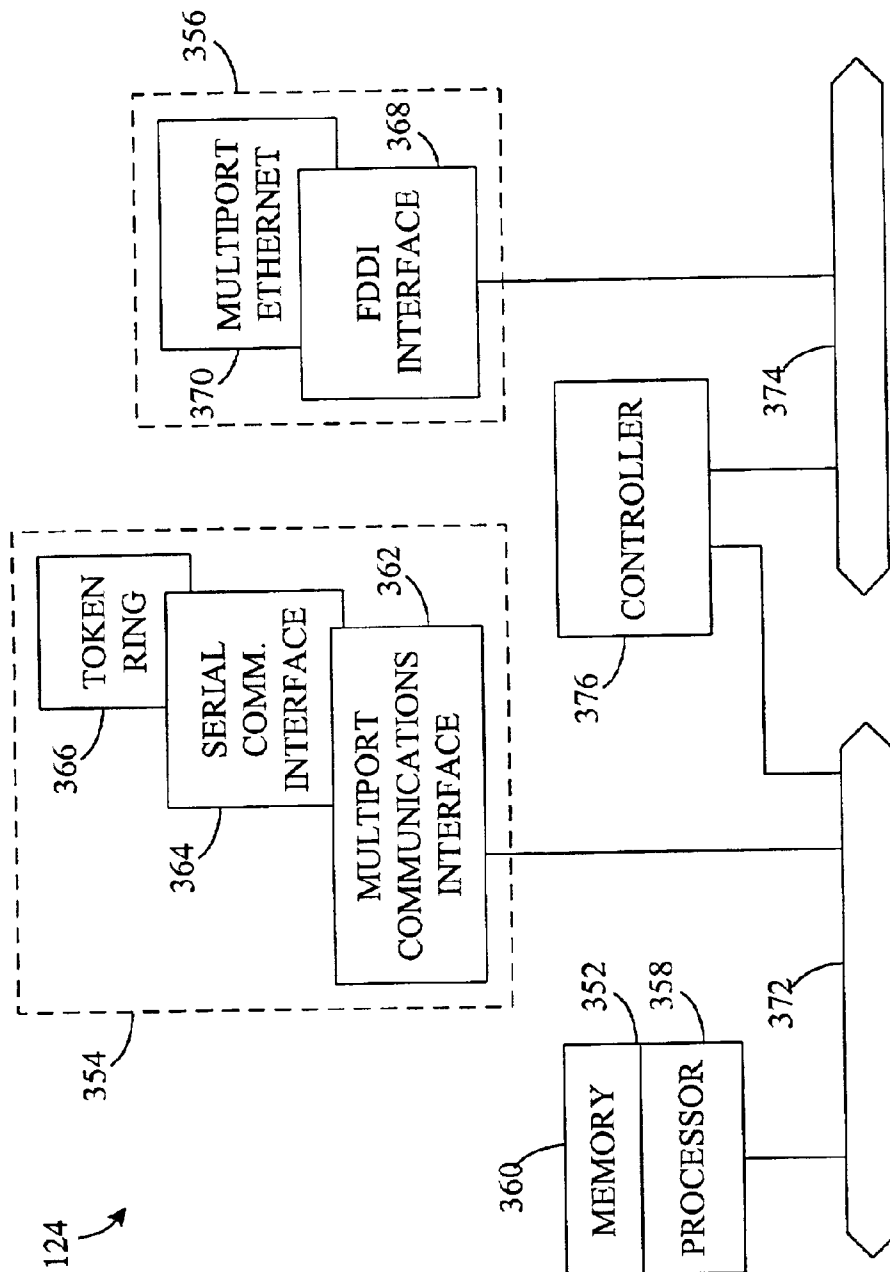


Fig. 3b

U.S. Patent

Aug. 23, 2005

Sheet 5 of 8

US 6,934,754 B2

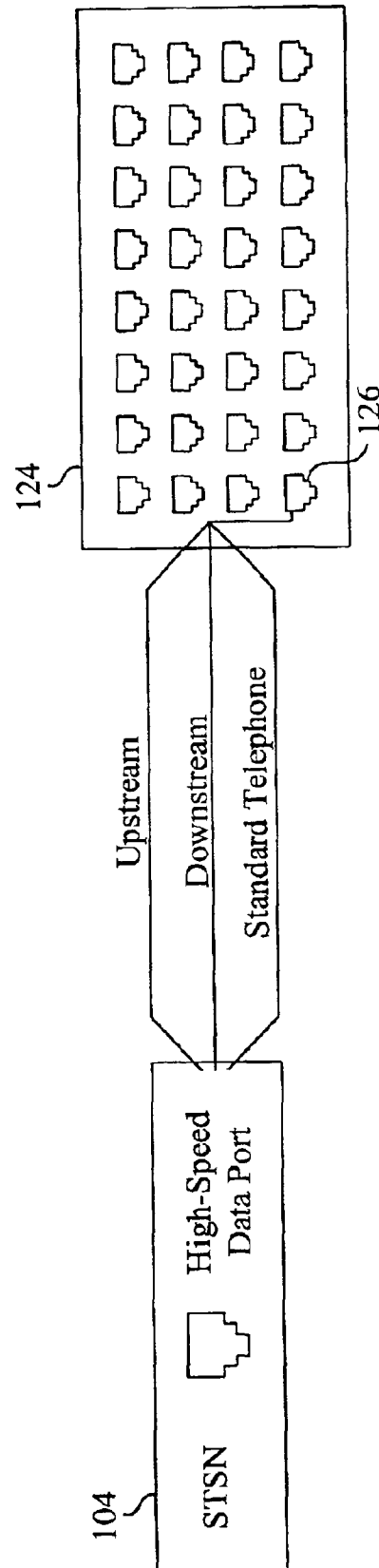


Fig. 4

U.S. Patent

Aug. 23, 2005

Sheet 6 of 8

US 6,934,754 B2

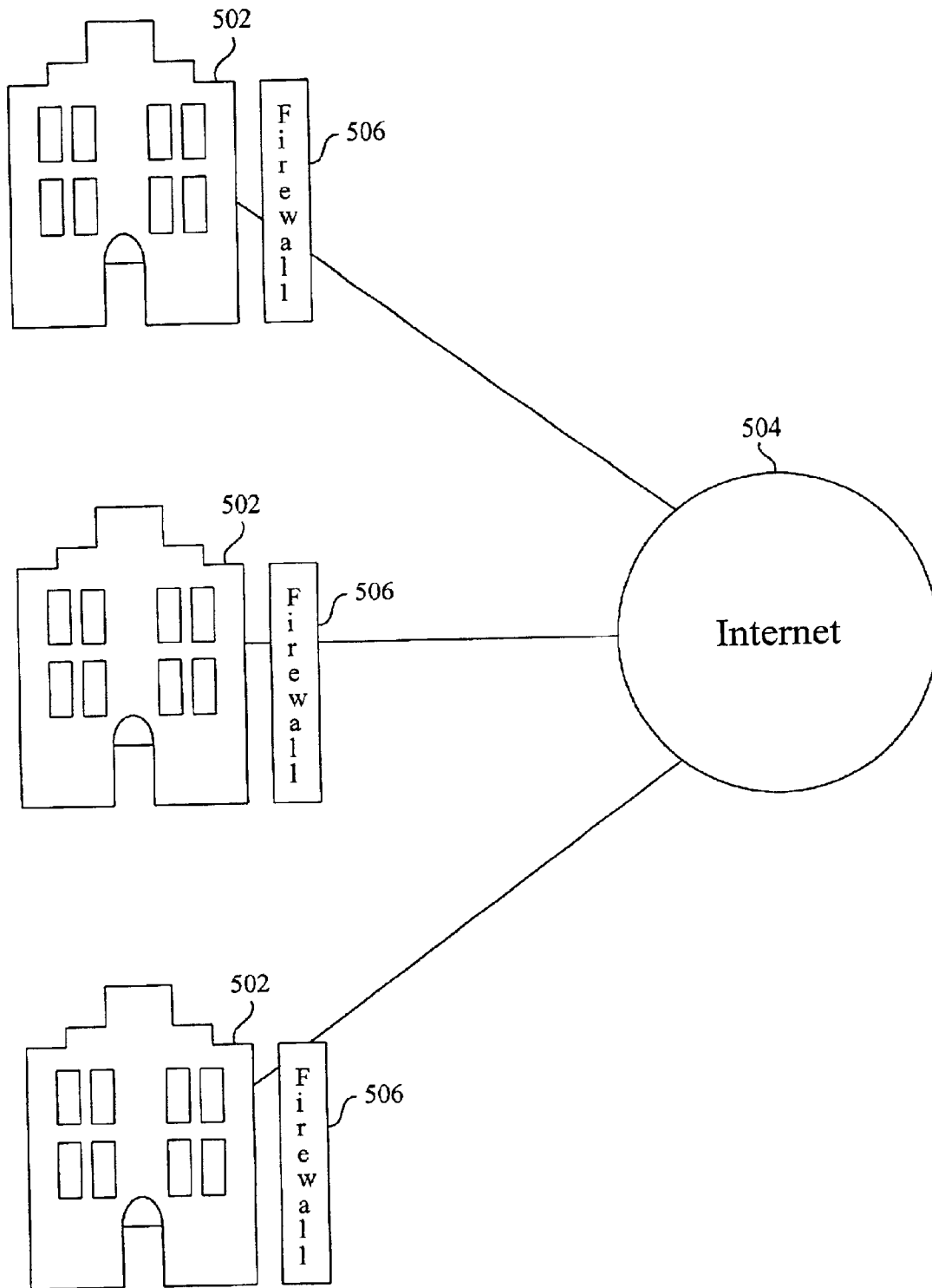


Fig. 5

U.S. Patent

Aug. 23, 2005

Sheet 7 of 8

US 6,934,754 B2

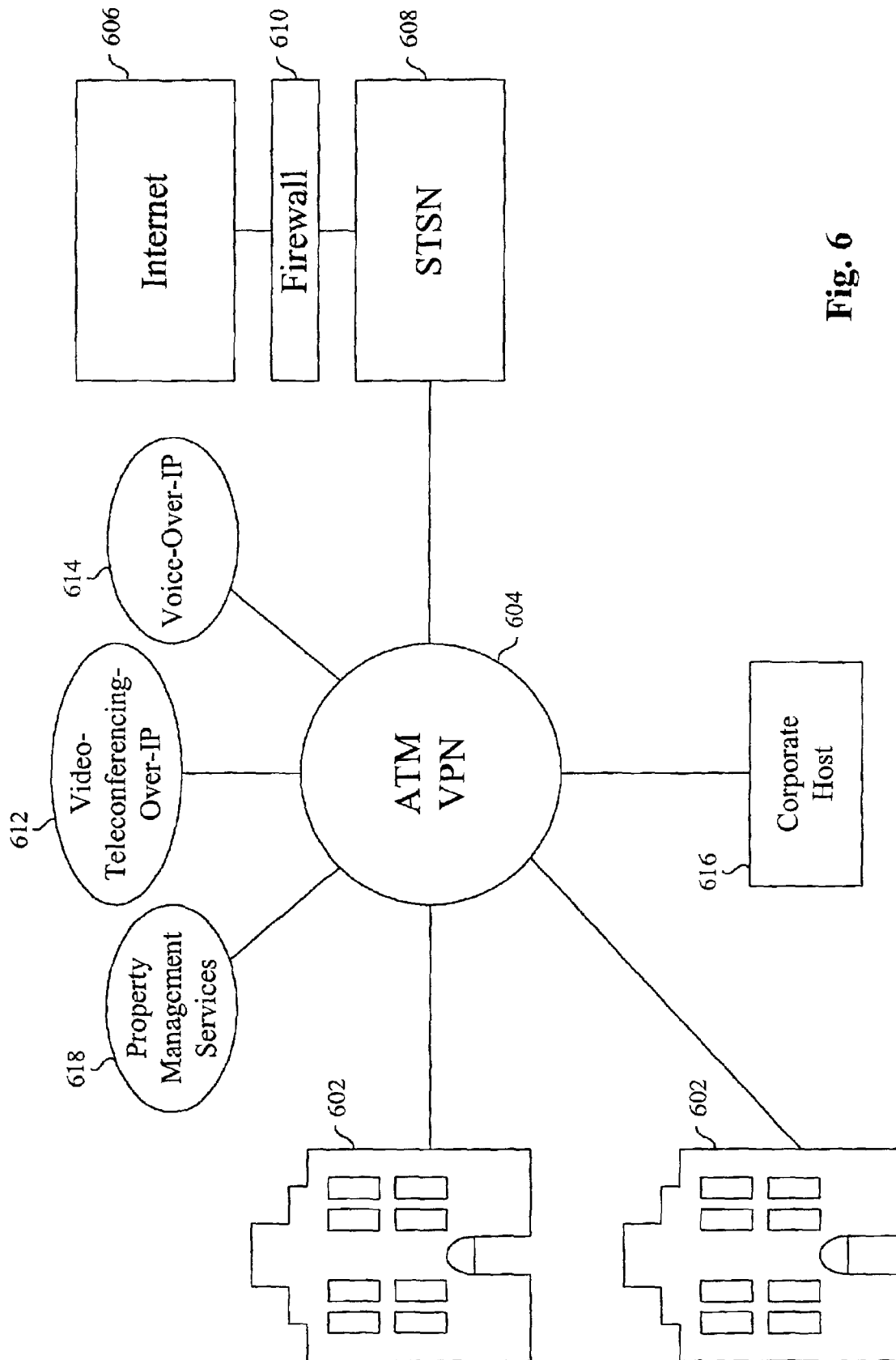


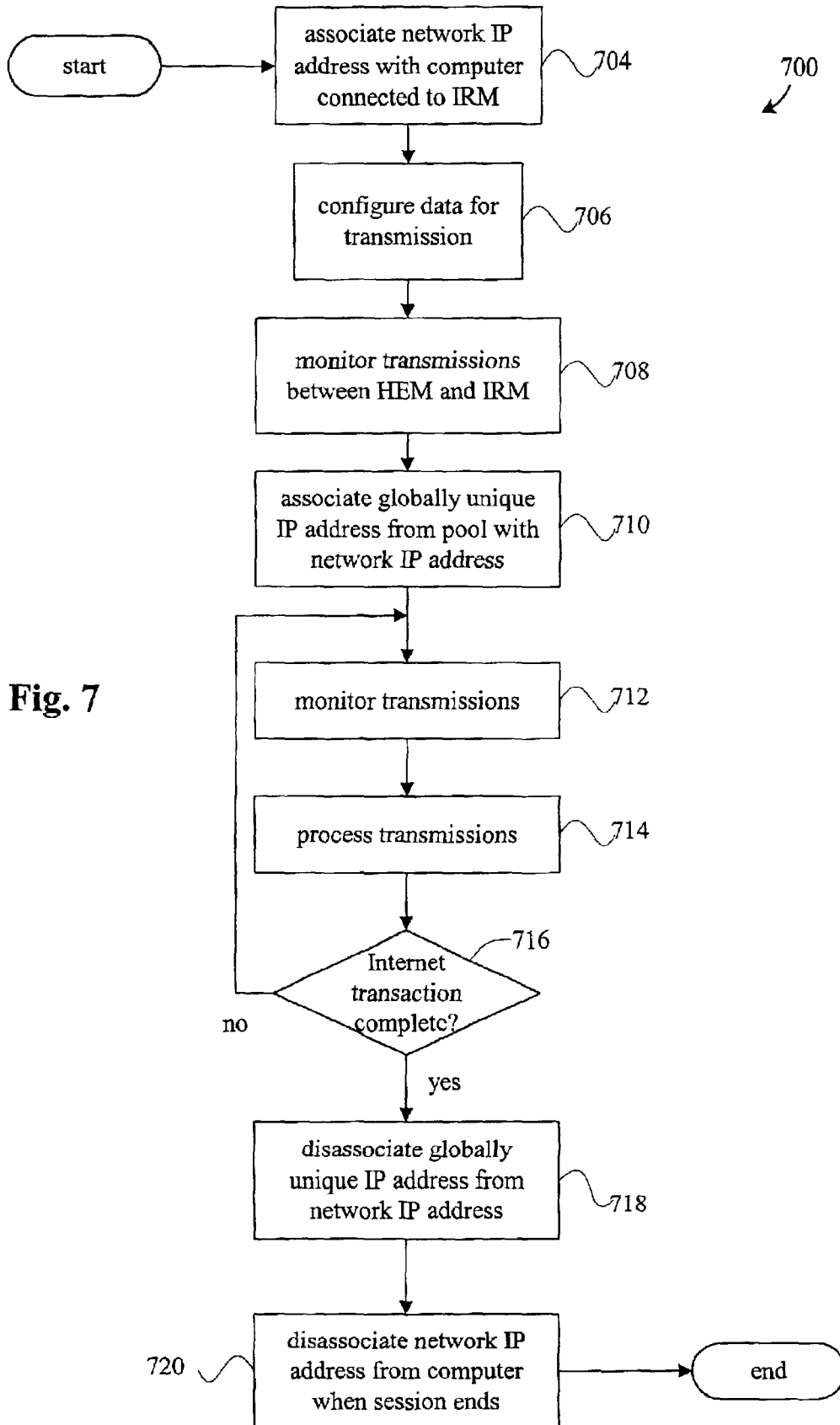
Fig. 6

U.S. Patent

Aug. 23, 2005

Sheet 8 of 8

US 6,934,754 B2



US 6,934,754 B2

1

METHODS AND APPARATUS FOR PROCESSING NETWORK DATA TRANSMISSIONS

RELATED APPLICATION DATA

The present application claims priority from U.S. Provisional Patent Application No. 60/194,354 for **METHODS AND APPARATUS FOR TAGGING HTML TRAFFIC** filed on Apr. 3, 2000, the entire disclosure of which is incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

The present invention relates to network communications and, more specifically, to methods for monitoring, tagging, and redirecting traffic in network communication systems.

Any business traveler who relies on network communications to maintain contact with clients and the home office appreciates the availability of fast and reliable data ports at remote locations such as airport lounges and hotel rooms. The hospitality industry has only recently begun to understand the necessity of providing such high speed data connections to business travelers. In fact, given the explosive growth of network technologies and the corresponding dependence of the business professional on such technologies, hotels which do not move to provide high speed connectivity in guest rooms comparable to the typical office environment will likely lose a substantial portion of their business to hotels which do.

Unfortunately, many hotel rooms are not currently wired to accommodate high speed data traffic. That is, prior to 1990, virtually all hotel rooms were wired to provide only basic telephone service. As late as 1995, less than 10% of hotel rooms were wired to handle standard Ethernet data speeds. Even today, while the major players in the hospitality industry are searching for high speed connectivity solutions, the vast majority of hotel guest and conference rooms are still wired with low quality, single pair connections. One obvious solution would be to completely rewire all of the guest and conference rooms in each hotel facility to provide the desired data transmission capabilities. However, given the prohibitive cost of such an undertaking, a less costly solution would be desirable.

Even if such a costly rewiring were undertaken, there are other problems which are not addressed by an infrastructure upgrade. For example, even if a high speed connection to the hotel's host is provided, it will often be the case that a guest's laptop computer would be incompatible with the hotel network in some way. Thus, each guest's laptop must be configured appropriately in order to communicate with the network and with the Internet beyond. This would likely involve loading special software onto a guest's laptop each time the guest wants to go online. Not only would such a process be cumbersome and annoying to the hotel guest, it may also be unacceptable from the guest's point of view in that reconfiguring the laptop may interfere with the current configuration in undesirable ways.

Neither does a costly wiring upgrade address the administrative and security issues related to providing Internet access via a hotel host. That is, high speed Internet access for hotel guests requires a network at the hotel property and some sort of connection between the hotel network and the Internet, e.g., a T1 or T3 line. A firewall at each hotel property would also be required to protect the internal network from unauthorized access. The existence of the firewall at each property, in turn, requires that most of the control and administration of the local network be per-

2

formed at the hotel property rather than remotely, thus representing an undesirable redundancy of administrative functions.

Another administrative difficulty related to maintaining each hotel property as a separate Internet host involves the management of IP addresses. Ranges of globally unique 32-bit IP addresses are issued to organizations by a central Internet authority. These addresses are organized in a four octet format. Class A IP addresses are issued to very large organizations and employ the first of the four octets to identify the organization's network and the other three to identify individual hosts on that network. Thus, a class A address pool contains nearly 17 million (2^{24}) globally unique IP addresses. With class B addresses, the first two octets are used to identify the network and the last two to identify the individual hosts resulting in 64,000 (2^{16}) globally unique IP addresses for each organization. Finally, with class C addresses, the first three octets are used to identify the network and the last octet to identify the individual hosts resulting in only 256 (2^8) globally unique IP addresses for each organization.

Unfortunately for many medium to large size organizations (1,000 to 10,000 hosts), it has become very difficult, if not impossible, to obtain anything other than a class C address for their networks due to the fact that the class A and B address spaces have been almost entirely locked up. This problem has been addressed to some extent by the use of a Network Address Translation (NAT) protocol. According to such a protocol, when a local host on an organization's network requests access to the Internet, it is assigned a temporary IP address from the pool of globally unique IP addresses available to the organization. The local host is identified by the globally unique address only when sending or receiving packets on the Internet. As soon as the local host disconnects from the Internet, the address is returned to the pool for use by any of the other hosts on the network. For additional details on the implementation of such a protocol please refer to K. Evegang and P. Francis, *The IP Network Address Translator (NAT), Request for Comments "RFC" 1631*, Cray Communications, NTT, May 1994, the entirety of which is incorporated herein by reference for all purposes.

Such dynamic assignment of IP addresses might be sufficient for certain organizations as long as the number of simultaneous users which require access to the Internet remains below the maximum of 256. However, if, for example, a 1200 room hotel were hosting an Internet technologies seminar it would be extremely likely that the demand for Internet access would exceed the available address pool. All of this also assumes that a major hotel chain would be able to obtain a complete class C pool of addresses for each of its properties; not necessarily a reasonable assumption.

It is therefore desirable to provide methods and apparatus by which each of the properties in a major hotel chain may provide high speed Internet access to each of its guest rooms in a secure, inexpensive, and reliable manner without undue administrative burdens on the individual properties.

SUMMARY OF THE INVENTION

According to the present invention, methods and apparatus are provided which make use of existing hotel wiring infrastructures to provide secure, high speed data and Internet access to each of the guest rooms in a hotel property. According to one embodiment of the invention, each guest room in the hotel is interconnected via the hotel's current wiring infrastructure into a local network. When a guest

US 6,934,754 B2

3

wishes to access the Internet, he connects his laptop to an in-room module installed in each guest room which temporarily assigns a "fake" local IP address to the guest's laptop. The "fake" local IP address is associated with the in-room module and is unique on the hotel's local network. The address is "fake" in that it is not a valid Internet address and in that it replaces the laptop's own real IP address. The assigned local IP address uniquely identifies the guest's laptop on the hotel network while that laptop remains connected to the in-room module.

A headend module in the hotel handles packet routing and provides access to the Internet. In facilitating access to the Internet, the headend module temporarily assigns globally unique IP addresses from a pool of, for example, class C addresses to in-room modules in individual guest rooms in response to requests for Internet access from those rooms. An assigned IP address remains dedicated to a particular in-room module (and thus the associated guest's computer) for the duration of the Internet transaction. Upon termination of the transaction, the globally unique IP address is disassociated from the in-room module and put back into the pool for use in facilitating a later Internet transaction from any of the hotel's rooms.

According to another embodiment of the invention, the local networks of a number of hotels are interconnected via a remote server thereby forming a private wide area network, or a virtual private network. The operation of the virtual private network to provide high speed data and Internet access to individual guest rooms is similar to the process described above except that the "fake" IP address of the in-room modules are unique over the entire virtual private network, and the temporary assignment of globally unique IP addresses is performed by the remote server rather than the hotel headend. This is advantageous in that it is contemplated that the remote server has a larger pool of such addresses associated therewith than an individual hotel network might be able to procure (e.g., a class B address pool).

Thus, because the IP address needs of all of the hotels in the virtual private network are spread out over the entire installed base of the remote server, bursts of need at any one property which exceed the capacity of a single class C address pool may be accommodated. The virtual private network embodiment of the present invention also has the advantage that firewall security and other network administrative functions may be centralized and performed remotely without compromising the security of any individual hotel network.

According to various additional embodiments, the processing power of the in-room module of the present invention is employed to monitor the data being transmitted to and from the connected computer, and to provide a variety of functions based on the nature of the transmissions being monitored. For example, the in-room module may determine the destination of data transmissions from the computer by parsing and HTML string or looking at the TCP connection. Then, depending on the destination, the in-room module can perform various functions such as tagging the transmissions, framing pages sent to the computer in response to the transmission, or redirecting the transmissions for processing at some other location, e.g., an associated server.

Thus, according to the present invention, methods and apparatus are provided for providing access to a network via a first one of a plurality of network access nodes in the network. The network access nodes each have a network address associated therewith which is unique on the

4

network, the first network access node having a first network address associated therewith. The first network address is associated with a first computer while the first computer is connected to the first network access node thereby providing access to the network. Transmissions associated with the first computer are monitored to determine address information. The transmissions are then processed in response to the address information.

A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a hotel according to a specific embodiment of the invention;

FIG. 2 is a flowchart illustrating a method for providing high speed data and Internet access to guest rooms in a hotel according to a specific embodiment of the invention;

FIGS. 3a and 3b are more detailed block diagrams of the in-room module and head-end module of FIG. 1;

FIG. 4 is a block diagram illustrating the combination of half duplex data and standard telephone data on a single pair of conductors according to a specific embodiment of the invention;

FIG. 5 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in hotels according to another specific embodiment of the invention;

FIG. 6 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in hotels according to yet another specific embodiment of the invention; and

FIG. 7 is a flowchart illustrating providing network access and the selective processing of data transmissions according to a specific embodiment of the present invention.

DESCRIPTION OF SPECIFIC EMBODIMENTS

FIG. 1 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a hotel network 100 according to a specific embodiment of the invention. In each guest room 102 is an in-room module (IRM) 104 by which a telephone 106 and a guest's laptop computer 108 may be connected to the hotel's wiring infrastructure. According to a specific embodiment, IRM 104 is plugged directly into the room's phone jack and has at least two additional ports, one for the room's telephone, e.g., an RJ-11 jack, and one for the guest's laptop, e.g., an RJ-45 Ethernet port. According to various embodiments, IRM 104 performs a number of functions including, for example, combining and separating Ethernet data and standard telephone signals for transmission over the hotel's wiring infrastructure. According to other embodiments and as discussed below, IRM 104 is configured to receive control information from a central location for automated control of various room environmental parameters, e.g., temperature and lighting. According to still other embodiments, IRM 104 is configured to receive a wide variety of other types of data such as, for example, digital audio and video for presentation in the guest room, or a wide variety of other information services.

Transmission line 110 connects IRM 104 to the hotel's head-end 112 via any of a wide variety of infrastructures. In the example shown, standard telephone transmission line 110 connects IRM 104 to head-end 112. It will be understood, however, that the wiring between IRM 104 and

US 6,934,754 B2

5

head-end **112** may take other forms such as, for example, a four-conductor Ethernet transmission line. Head-end **112** comprises a main distribution frame (MDF) punch down block **116**, a public branch exchange (PBX) punch down block **118**, and a public branch exchange (PBX) **120**. Interposed between punch down blocks **116** and **118** is an HEM punch down block **122**. Standard telephone signals pass through punch down block **122** to PBX **120** while half duplex Ethernet data packets are transmitted and received by head-end module (HEM) **124**. This splitting of the telephone signals and data packets may be effected by any of a variety of filtering techniques as represented by filters **119** and **121**. As will be understood, these filters may be incorporated into punch down block **122** or be separate devices. Additional filtering may also be provided to further mitigate undesirable effects from having voice and data on the same lines. Such filtering is also represented by filters **119** and **121**. It will be understood that the configuration shown is merely for illustrative purposes and is not intended to limit the scope of the invention.

Depending on the configuration of the present invention, HEM **124** performs a variety of functions and, according to some embodiments, can be thought of as an enhanced router with additional capabilities programmed into its operating system. That is, according to such embodiments, HEM **124** serves as a switch which routes data packets to and from IRMs **104**, and serves as the other end of the communications to and from IRMs **104** in which Ethernet data and phone signals are combined over single twisted pair technology. According to other alternative embodiments, HEM **124** handles address translation and assignment, controls network access, and serves as a bridge for Ethernet data transmitted over the hotel's single twisted pair infrastructure. HEM **124** has a plurality of ports **126** each of which communicates with a corresponding IRM **104**. This communication may be individually monitored and controlled (by either the IRM or the HEM) thus allowing central hotel management of billing and access as well as the ability to generate reports for troubleshooting purposes.

Each IRM **104** (and thus the corresponding HEM port **126**) has a fixed IP address which may be configured using any of a variety of network management protocols such as, for example, the Simple Network Management Protocol (SNMP). If the guest's computer connected to a particular IRM **104** does not have its own internal IP address, the fixed IP address of the corresponding IRM **104**/HEM port **126** is assigned to the guest's computer using the Dynamic Host Configuration Protocol (DHCP) to facilitate access to network **100**. If the guest's computer already has its own internal IP address, address translation is performed between the computer's internal IP address and the fixed IP address of the IRM **104**/HEM port **126**. According to various embodiment of the invention, this address translation may be performed by either IRM **104** or HEM **124**. HEM **124** has a small boot ROM (not shown) for basic IP communications and a large flash ROM (not shown) for fully functional software and configuration data. This allows for remote software upgrades using, for example, an encrypted protocol riding on top of IP.

FIG. 2 is a flowchart **200** illustrating a method for providing high speed data and Internet access to guest rooms in a hotel using the system of FIG. 1. When a guest's computer connects to an IRM in any one of the guest rooms, the network IP address associated with that IRM is associated with the computer (**204**). As discussed above, this association could mean a DHCP assignment of the network IP address to the guest's computer where the computer did

6

not already have an internal IP address. It could also mean that the internal IP address of the computer is translated into the network IP address. This address assignment/translation may be effected by either the IRM or the HEM. In addition, it will be understood that depending on where the assignment/translation occurs it may precede or follow **206** described below. The network IP address is associated with the guest's computer while it remains connected to the IRM.

Where the transmission line connecting the IRM to the hotel network comprises a single twisted pair of conductors, the data communications between the IRM and the HEM are configured so that they may be transmitted substantially simultaneously over the single twisted pair with the standard telephone signals from the phone in the guest room (**206**). A specific technique by which this configuration is effected is described below with reference to FIGS. **3a** and **4**.

Once the connection is established, the communications between the IRM and the HEM are monitored either periodically or continuously for a variety of purposes (**208**). This information may be used by the hotel for billing purposes or for troubleshooting and improving the reliability of the hotel network.

If an Internet transaction is requested by the guest's computer, a globally unique IP address from a pool of such addresses is temporarily associated with the network IP address currently associated with the guest's computer using, for example, a network address translation protocol (**210**). As discussed above, the pool of addresses could be, for example, class A, B, or C addresses. As will be discussed below with reference to FIGS. **5** and **6**, the temporary association of the globally unique IP address may be done by the HEM in the hotel or, according to another embodiment, by a remote server which interconnects one or more hotel properties in a wide area network. When the Internet transaction is complete (**212**), the globally unique IP address is disassociated from the network IP address and put back in the pool for use in facilitating subsequent Internet transactions from any of the hotel's guest rooms (**214**). The network IP address remains associated with the guest's computer until the session ends, e.g., the computer is disconnected from the IRM or powered down (**216**).

FIGS. **3a** and **3b** are more detailed block diagrams of IRM **104** and HEM **124** of FIG. 1, respectively. IRM **104** comprises connection circuitry for connecting the IRM to the room's standard telephone jack as well as the room's telephone and the guest's computer. According to various embodiments, the connection circuitry may include RJ-11 ports **302** for connecting to the phone and **303** for connecting to the wall jack, an Ethernet port **304**, a universal serial bus (USB) port **306** for connecting to the guest's computer, and an additional data port **307** for receiving various types of data. USB port **306** may, in some instances, prove more convenient than Ethernet port **304** in that certain network reconfiguration issues don't have to be dealt with. In addition, many business travelers often don't travel with the Ethernet dongle which is necessary for connecting their laptop's Ethernet port to a network Ethernet port. Thus, IRM **104** is operable to translate the laptop's transmissions to the Ethernet standard.

According to a specific embodiment, IRM **104** also includes transmission circuitry **308** for transmitting and receiving data on a single twisted pair of conductors of which the majority of hotel wiring infrastructures are comprised. According to one embodiment, a portion of transmission circuitry **308** is implemented according to the home PNA (Phone-line Networking Alliance) standard which

US 6,934,754 B2

7

allows half duplex data and phone signals on the same line as illustrated by the diagram of FIG. 4. According to the home PNA standard, data transmissions from IRM 104 to a port 126 of HEM 124 and transmissions from the HEM to the IRM are alternated at a frequency in the range of 4–9 MHz, e.g., 7.5 MHz. Because standard phone signals exist at a relatively low frequency compared to the home PNA modulation frequency, all of the signals may easily exist on a single pair of wires.

According to a specific embodiment, transmission circuitry 308 is operable to associate the network IP address associated with IRM 104 with the guest's computer. That is, the address translation or assignment which allows the guest access to the local or wide area network is performed by the transmission circuitry in the IRM. According to a more specific embodiment, transmission circuitry 308 includes a processing unit 309 based on RISC microprocessor which performs the address translation, the combining and separation of signals for transmission to the headend, and the routing of the received signals to the appropriate IRM port. According to a specific embodiment, processing unit 309 comprises an Intel 80960VH and the appropriate support circuitry.

According to another specific embodiment, IRM 104 also includes control circuitry 310 for receiving control information via the hotel's network for controlling one or more control systems 311 proximate to the IRM. Such control systems may include, for example, the room's temperature control, lighting, and audio systems. In one embodiment, the control circuitry includes conversion circuitry 312 for converting the received control information into the necessary control signals for actually controlling the in-room control systems. The conversion circuitry may include, for example, an RF transmission element 314 (e.g., an antenna) for transmitting RF control signals to the various control systems. According to an alternative embodiment, conversion circuitry 312 includes an infrared transmission element (e.g., an IR diode) for transmitting infrared control signals to various control systems.

Transmission circuitry 308 (using processor 309) discriminates between the various data it receives and directs it to the appropriate port on IRM 104 according to address information in data packet headers. According to a specific embodiment, digital audio and video may be transmitted to individual rooms via the system described herein. The digital audio and video are directed to additional data port 307 to which an audio and/or video system may be connected for presenting the transmitted content. In this way, an ambience may be set for the guest's arrival. In addition, the guest could select a wide variety of entertainment and information services via the hotel network which may then be transmitted to the guest's room via the auxiliary data port 307 on IRM 104.

Specific embodiments of IRM 104 also include an LED or LCD display 316 on which status and other information may be communicated to the occupant of the guest room whether or not they are currently connected. For example, before a connection is made, display 316 could be used to inform the hotel guest of all of the services available through IRM 104 as well as instructions for connecting to IRM 104. Other information such as stock quotes and weather information may also be presented continuously or periodically. Once connected, display 316 could communicate the status of the connection as well as the time connected and current connection charges. It will be understood that a wide variety of other information may be presented via display 316.

IRM 104 may also include an array of individual colored LEDs 318 which provide information to the user. Such

8

LEDs may indicate, for example, the connection status of the IRM, i.e., whether it is connected to the HEM, using red or green LEDs. LEDs 318 may also be configured to indicate a purchase status to the user. That is, because connection services are often purchased in 24 hour blocks, LEDs 318 may indicate to the user whether she is operating within a block of time which has already been paid for (green), whether the end of the current block is approaching (yellow), or whether she has already entered the next time block (red). LEDs 318 could also indicate which type of connection the user has established, e.g., USB or Ethernet.

As mentioned above and as shown in FIG. 3b, HEM 124 may be thought of as an enhanced router which routes data packets to and from IRMs 104, controls network access, serves as a bridge for Ethernet data transmitted over the hotel's single twisted pair infrastructure, and, according to some embodiments, handles address translation and assignment. According to various embodiments, the functionalities of HEM 124 may be implemented using functionalities available in, for example, a 2611 router and a Catalyst 2900 Ethernet switch from Cisco Systems, Inc. HEM 124 includes a master central processing unit (CPU) 352, low and medium speed interfaces 354, and high-speed interfaces 356. When acting under the control of appropriate software or firmware, the CPU 352 is responsible for such router tasks as routing table computations and network management. It may also be responsible for controlling network access and transmissions, etc. It preferably accomplishes all these functions under the control of software including an operating system (e.g., the Internet Operating System (IOS®) of Cisco Systems, Inc.) and any appropriate applications software. CPU 352 may include one or more microprocessor chips 358. In a specific embodiment, a memory 360 (such as non-volatile RAM and/or ROM) also forms part of CPU 352. However, there are many different ways in which memory could be coupled to the system.

The interfaces 354 and 356 are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receipt of data packets over the network and sometimes support other peripherals used with HEM 124. The low and medium speed interfaces 354 include a multiport communications interface 362, a serial communications interface 364, and a token ring interface 366. The high-speed interfaces 356 include an FDDI interface 368 and a multiport Ethernet interface 370. Preferably, each of these interfaces (low/medium and high-speed) includes (1) ports for communication with the appropriate media, (2) an independent processor, and in some instances (3) volatile RAM. The independent processors control such communications intensive tasks as packet switching, media control and management. By providing separate processors for the communications intensive tasks, this architecture permits the master microprocessor 352 to efficiently perform routing computations, network diagnostics, security functions, etc.

The low and medium speed interfaces 354 are coupled to the master CPU 352 through a data, control, and address bus 372. High-speed interfaces 356 are connected to the bus 372 through a fast data, control, and address bus 374 which is in turn connected to a bus controller 376.

Although the system shown in FIG. 3b is one type of router by which the present invention may be implemented, it is by no means the only router architecture by which the present invention may be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc. would also be acceptable. Further, other types of interfaces and media could also be used with the router.

US 6,934,754 B2

9

Regardless of network device's configuration, it may employ one or more memories or memory modules (including memory **360**) configured to store program instructions for the network operations and network access and control functions described herein. The program instructions may specify an operating system and one or more applications, for example. Such memory or memories may also be configured to store, for example, control information for controlling in-room control systems, etc.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). The invention may also be embodied in a carrier wave travelling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Referring back to FIG. **3b**, HEM **124** has a plurality of ports **126** each of which communicates with a corresponding IRM **104**. HEM **124** has the ability to sense when any of ports **126** are being used so that the hotel may bill the user accordingly. This monitoring feature is also useful for technical support, network bandwidth requirement estimates, billing estimates, and buying pattern data. HEM **124** also has the capability of enabling and disabling individual ports **126**. Where network **100** is part of a wide area network (as discussed below), the monitoring, enabling, and disabling of ports **126** may be done from a remote server at the center of the WAN.

As described above, each HEM port **126** (and thus the corresponding IRM **104**) has a fixed IP address which may be configured using any of a variety of network management protocols such as, for example, SNMP. The fixed IP address of the HEM port **126** and the IRM **104** is assigned to the guest's computer using DHCP. Alternatively, an address translation is performed between the computer's internal IP address and the fixed IP address of IRM **104**/HEM port **126**. HEM **124** has a small boot ROM **378** for basic IP communications and a large flash ROM **380** for fully functional software and configuration data. This allows for remote software upgrades using, for example, an encrypted protocol riding on top of IP.

According to various embodiments, HEM **124** also comprises transmission circuitry **316** for transmitting and receiving data on a single twisted pair of conductors. Thus, the Ethernet data which has been combined with the standard telephone signals at IRM **104** may be picked off and reconfigured for transmission according to standard Ethernet techniques. Also, data headed to IRM **104** may be combined for transmission over the single twisted pair. As with transmission circuitry **308**, transmission circuitry **316** may be implemented according to the home PNA standard.

FIG. **5** is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a chain of hotels **502** according to one embodiment of the invention. Using the internal infrastructure described above with ref-

10

erence to FIG. **1**, each hotel **502** has a local area network (LAN) (not shown) which provides direct access to the Internet **504** for each of its guest rooms. According to this embodiment, each hotel **502** must provide its own security in the form of a firewall **506** for the protection of its LAN.

FIG. **6** is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a chain of hotels **602** according to another embodiment of the invention. Using the internal infrastructure described above with reference to FIG. **1**, each hotel **602** has a LAN (not shown) which is then connected with other LANs in the other hotels **602** to form a wide area network (WAN) referred to herein as a virtual private network (VPN) **604**. According to a specific embodiment, VPN **604** is built on an optical fiber backbone employing asynchronous transfer mode (ATM) technology to transmit data packets. It will be understood however that any of a variety of transmission protocols and infrastructures may be employed to transmit data in such a network without departing from the scope of the present invention. Such protocols may include but are not limited to frame relay, Ethernet, and FDDI. Data are configured in the appropriate format as they leave each hotel **602** by a framer (not shown) which may be part of or associated with each hotel's router or file server.

The embodiment of FIG. **6** provides several advantages over the embodiment described above with reference to FIG. **5**. High speed access to the Internet requires some form of connection to the Internet such as, for example, a T1 or T3 line. Not only does such a connection require a hardware infrastructure to support it, it also necessitates some form of protection for the network in the form of, for example, a firewall. Thus, if each hotel property in a hotel chain were to be directly connected to the Internet (as shown in FIG. **5**), each property would need to have its own network hardware infrastructure, firewall, and the technical and administrative staff and functions to support the same. By contrast, with VPN **604**, access to the Internet **606** is provided via a single network center (represented by remote network operation center (NOC) server **608**) at which one or more firewalls **610** and any other necessary networking hardware and equipment may be located and managed. According to a specific embodiment, a redundant network center is provided in a different city than the first against the event that one or the other goes down.

Having each hotel property directly connected to the Internet is problematic for effecting control of the hotels from a central location. That is, the more each hotel LAN is amenable to control from a central location, the more vulnerable it is to hacking. With VPN **604**, security is complete and centralized control is virtually unlimited. This makes things like remote software upgrades convenient thus eliminating what might otherwise be significant field service costs. In addition, because much of the equipment is centrally located, the costly redundancy of equipment and support functions at each hotel property made necessary by the embodiment of FIG. **5** is avoided.

Another important benefit of VPN **604** relates to the management of globally unique IP addresses. As mentioned above, there is a paucity of pools of globally unique IP addresses which are sufficiently large to accommodate each host on the networks of most medium to large size organizations. For example, one pool of class C addresses accommodates less than 256 simultaneous users on a network. This might be sufficient at most hotels much of the time, but it is clear that there are foreseeable circumstances where it would not be. For example, as mentioned above, if a 1200 room hotel hosted an Internet technologies seminar it is highly

US 6,934,754 B2

11

likely that such a pool of addresses would not be sufficient. In addition, this scenario makes the assumption that each property in a hotel chain (some comprising over 1000 properties) could procure a pool of class C addresses.

VPN 604 addresses this problem in that it spreads the IP address needs of each of the hotel properties over the resources of the entire wide area network. Thus, for example, a single class B pool of addresses might be used to accommodate all of the Internet access needs of an entire hotel chain even where the total number of rooms in the chain far exceeds the number of available globally unique IP addresses. That is, large bursts of IP address needs may occur simultaneously at dozens of the hotel properties without exhausting the nearly 64,000 globally unique addresses available in the class B pool.

Other secure services may also be provided via VPN 604. For example, video teleconferencing-over-IP 612 and voice-over-IP communications 614 may be provided to hotel guests. Moreover, by arranging access to VPN 604 by corporate hosts 616, individual employees of those corporations can have secure access to their employer's network from remote locations. Other services such as, for example, property management services 618 may be provided to the management of hotels 602.

According to a specific embodiment, the processing power of the in-room module of the present invention, e.g., IRM 104 of FIG. 3a, is employed to effect a variety of advanced IP and HTML processing functions. According to various embodiments, such functions may relate to the monitoring, tagging, and redirection of network traffic. One such function relates to the manner in which web sites and portals track the source of traffic referred to their sites.

Many e-commerce web sites offer a share of their revenues to sites which refer user traffic. These referrals are typically accomplished through links to the e-commerce sites embedded in the pages of the referring site. Traffic referred by such mechanisms typically includes an affiliate tag identifying the referring site. It is through the use of affiliate tags that the target e-commerce sites track the source of referred traffic and determine the compensation owed the various referring affiliate sites.

One shortcoming of the above-described approach relates to the fact that the revenue opportunity may be lost by the referring site if the user employs some other mechanism than the provided link to access the target site. For example, if the user simply types the target site URL directly into his browser, the request is not tagged as originating from the affiliate site, even where the linking page of the affiliate site is currently being viewed by the user. Therefore, according to a specific embodiment of the invention, the IRM is configured to monitor requests originating from the associated computer and add affiliate link ID tags to appropriate requests whether they originated from selection of a hyperlink or direct typing of the URL.

More generally, the IRM of the present invention may be configured to monitor the traffic originating from the connected host and process the request in accordance with a predetermined protocol depending on the nature of the traffic being monitored. That is, because of the processing power in the IRM and the fact that only one computer is typically associated with each IRM, the traffic associated with the computer can be analyzed in very detailed ways, far more detailed in fact than is practicable for the traffic flowing through a typical network node, e.g., a router, which may correspond to hundreds or even thousands of user.

FIG. 7 is a flowchart 700 illustrating another method for providing high speed data and Internet access to guest rooms

12

in a hotel using the system of FIG. 1. When a guest's computer connects to an IRM in any one of the guest rooms, the network IP address associated with that IRM is associated with the computer (704). As discussed above, this association could mean a DHCP assignment of the network IP address to the guest's computer where the computer did not already have an internal IP address. It could also mean that the internal IP address of the computer is translated into the network IP address. This address assignment/translation may be effected by either of the IRM and the HEM. In addition, it will be understood that depending on where the assignment/translation occurs it may precede or follow 706 described below. The network IP address is associated with the guest's computer while it remains connected to the IRM.

The data from the guest's computer are then configured for transmission over the hotel wiring infrastructure (706). So, for example, where the transmission line connecting the IRM to the hotel network comprises a single twisted pair of conductors, e.g., a standard phone line, the data communications between the IRM and the HEM are configured so that they may be transmitted substantially simultaneously over the single twisted pair with the standard telephone signals from the phone in the guest room. This may be accomplished, for example, using standard well know DSL techniques. Alternatively, where the hotel is more up-to-date and includes a network communications infrastructure, the data may be transmitted according to any of a wide variety of network transmission protocols, e.g., Ethernet.

Once the connection is established, the communications between the IRM and the HEM are monitored either periodically or continuously for a variety of purposes (708). This information may be used by the hotel for billing purposes or for troubleshooting and improving the reliability of the hotel network.

If an Internet transaction is requested by the guest's computer, a globally unique IP address from a pool of such addresses is temporarily associated with the network IP address currently associated with the guest's computer using, for example, a network address translation protocol (710). As discussed above, the pool of addresses could be, for example, class A, B, or C addresses. As will be discussed above with reference to FIGS. 5 and 6, the temporary association of the globally unique IP address may be done by the HEM in the hotel or, according to another embodiment, by a remote server which interconnects one or more hotel properties in a wide area network.

The data transmissions to and from each computer connected to each IRM may be monitored to effect a variety of functions (712). That is, because of the processing power available at the IRM, these data transmissions may be evaluated on any network protocol level, e.g., right down to an HTML string, to determine, for example, the destination to which the transmissions are directed or from which the transmissions originated. This information may then be used to process the transmissions in a wide variety of ways ranging from very simple to highly sophisticated (714).

Because of the processing power available in the IRM, the monitoring of the transmissions from the guest's computer may be accomplished with varying levels of sophistication. That is, information about these transmissions may be determined by evaluating the transmissions on any network communication protocol layer, i.e., from the physical to the application layer. So, for example, the IRM could identify the port to which a transmission is directed, e.g., port 80, by referring to the network layer. Alternatively, the IRM could identify the web site to which a transmission is directed by

US 6,934,754 B2

13

looking at the HTML string in a request. As will be understood, the possible ways in which the transmission may be monitored are limited only by the number of types of transmissions which could originate from or be directed to the guest's computer.

The way in which the transmissions may then be processed are similarly diverse. For example, if the transmissions are monitored to determine the destination of a web request, this information may be used in a variety of ways. Again for example, where an affiliate agreement exists between the destination site and the provider of the network services of the present invention, an affiliate tag may be associated with the transmissions to the destination site. This may be accomplished by appending the affiliate tag to the HTML string designating the destination site.

Alternatively, the information about the destination site could be employed to effect the generation of pop-up windows or the framing of web pages on the guest's computer with content relating in some way to the destination site. The content of such a frame or window might relate to the business of the destination site or that of a competitor. That is, if the computer user sends a request to the Coca-Cola® web site, the returned web pages could be displayed with a promotional offer from Coca-Cola® or an advertisement from Pepsi®.

The processing of the data transmission, whether it relates to tagging, framing, or some other type of processing may occur in the IRM itself, or may alternatively be accomplished at another network node (e.g., the HEM, or a local or remote server) by having the IRM redirect at least a portion of the transmissions through the processing node. So, for example, if the processing function relates to framing of web pages from specific destination sites, where transmissions from the guest computer are determined to be going to such a site, they may be redirected to the processing node which connects with the destination site and frames the pages it receives in response for presentation on the guest computer.

In general, it will be understood that the above-described examples of the monitoring and processing of transmissions to and from the guest computer are merely exemplary and that the present invention encompasses a great diversity of both functions.

Referring back to FIG. 7, when the Internet transaction is complete (or when a timeout period expires during which no packets are sent or received) (716), the globally unique IP address is disassociated from the network IP address and put back in the pool for use in facilitating subsequent Internet transactions from any of the hotel's guest rooms (718). The network IP address remains associated with the guest's computer until the session ends, e.g., the computer is disconnected from the IRM or powered down (720).

While the invention has been particularly shown and described with reference to specific embodiments thereof, it will be understood by those skilled in the art that changes in the form and details of the disclosed embodiments may be made without departing from the spirit or scope of the invention. For example, many of the embodiments described herein have been described with reference to hotels. It will be understood, however, that the techniques employed by the present invention may be applied to a variety of structures and institutions such as, for example, schools, office buildings, and the like. In addition, several embodiment described herein employ single twisted pair wiring which is the standard telephone wiring found in most buildings. However, it will be understood that the techniques described

14

herein may be implemented on any of a wide variety of wiring infrastructures including, for example, Ethernet and ATM systems. Therefore, the scope of the invention should be determined with reference to the appended claims.

What is claimed is:

1. A method for providing Internet access to a first computer via a first one of a plurality of network access nodes in a network using a plurality of globally unique IP addresses, the network access nodes each having a network address associated therewith which is unique on the network, the first network access node having a first network address associated therewith, the method comprising:

associating the first network address with the first computer while the first computer is connected to the first network access node thereby providing access to the network;

associating a first one of the globally unique IP addresses with the first network address for conducting an Internet transaction;

monitoring transmissions associated with the Internet transaction to determine address information;

processing the transmissions in response to the address information; and

disassociating the first globally unique IP address from the first network address upon termination of the Internet transaction, the first globally unique IP address then being available for association with any of the network addresses.

2. The method of claim 1 wherein the first computer has an internal IP address and associating the first network address with the first computer comprises translating the internal IP address of the first computer to the first network address.

3. The method of claim 1 wherein the first computer does not have an internal IP address and associating the first network address with the first computer comprises assigning the first network address to the first computer.

4. The method of claim 1 wherein associating the first globally unique IP address with the first computer comprises employing a network address translation protocol.

5. The method of claim 4 wherein the plurality of globally unique IP addresses comprises a pool comprising one of a plurality of class A, a plurality of class B, or a plurality of class C IP addresses.

6. The method of claim 1 wherein the network comprises a local area network and the associating and disassociating of the first globally unique IP address is done by a headend associated with the local area network.

7. The method of claim 1 wherein the network comprises a wide area network and the associating and disassociating of the first globally unique IP address is done by a remote server on the wide area network.

8. The method of claim 1 wherein associating the first network address with the first computer is done by the first network access node.

9. The method of claim 1 wherein portions of the network comprise a single pair of conductors, the method further comprising transmitting half duplex data and standard telephone signals substantially simultaneously over the single pair of conductors.

10. The method of claim 9 wherein transmitting the half duplex data comprises transmitting the half duplex data at a first frequency which is significantly higher than a second frequency at which the standard telephone signals are transmitted.

11. The method of claim 1 wherein monitoring and processing the transmissions is done by the first network access node.

US 6,934,754 B2

15

12. The method of claim 1 wherein monitoring the transmissions comprises parsing an HTML string associated with the transmissions.

13. The method of claim 1 wherein monitoring the transmissions comprises monitoring network layer information associated with the transmissions.

14. The method of claim 1 wherein monitoring the transmissions comprises monitoring any of a plurality of network communication protocol layers associated with the transmissions.

15. The method of claim 1 wherein processing the transmissions comprises associating an affiliate tag with the transmissions where the transmissions correspond to an affiliate.

16. The method of claim 15 wherein associating the affiliate tag comprises appending the affiliate tag to an HTML string associated with the transmissions.

17. The method of claim 1 wherein processing the transmissions comprises generating content for presentation on the first computer.

18. The method of claim 17 wherein the transmissions relate to a first entity, the content also relating to the first entity.

19. The method of claim 17 wherein the transmissions relate to a first entity, the content relating to a second entity in competition with the first entity.

20. The method of claim 17 further comprising presenting the content on the first computer in a pop-up window.

21. The method of claim 17 further comprising presenting the content on the first computer in a frame around at least one HTML page corresponding to the transmissions.

22. The method of claim 1 wherein processing the transmissions comprises redirecting the transmissions to a server to be processed.

16

23. The method of claim 22 wherein processing the transmissions comprises framing HTML pages to be presented on the first computer.

24. The method of claim 22 wherein processing the transmission comprises generating a pop-up window to be presented with HTML pages on the first computer.

25. A method for providing Internet access to a first computer via a first one of a plurality of network access nodes in a plurality of networks using a plurality of globally unique IP addresses, the network access nodes each having a network address associated therewith which is unique among the plurality of networks, the first network access node having a first network address associated therewith, the method comprising:

interconnecting the plurality of networks with a remote server thereby forming a wide area network, the globally unique IP addresses being associated with the remote server;

associating the first network address with the first computer while the first computer is connected to the first network access node;

associating a first one of the globally unique IP addresses with the first network address for conducting an Internet transaction;

monitoring transmissions associated with the Internet transaction to determine address information;

processing the transmissions in response to the address information; and

disassociating the first globally unique IP address from the first network address upon termination of the Internet transaction, the first globally unique IP address then being available for association with any of the network addresses.

* * * * *

EXHIBIT 2

(12) **United States Patent**
West et al.

(10) **Patent No.:** **US 6,996,073 B2**
(45) **Date of Patent:** **Feb. 7, 2006**

(54) **METHODS AND APPARATUS FOR
PROVIDING HIGH SPEED CONNECTIVITY
TO A HOTEL ENVIRONMENT**

(56) **References Cited**

U.S. PATENT DOCUMENTS

(75) Inventors: **William B. West**, Salt Lake City, UT
(US); **Wallace Eric Smith**, Lindon, UT
(US); **Steven R. McDaniel**, Salt Lake
City, UT (US)

(73) Assignee: **iBAHN General Holdings
Corporation**, South Jordan, UT (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 56 days.

5,790,548 A	8/1998	Sistanizadeh et al.	370/401
5,793,763 A	8/1998	Mayes et al.	370/389
5,812,819 A	9/1998	Rodwin et al.	395/500
5,835,725 A	11/1998	Chiang et al.	395/200.58
6,011,782 A *	1/2000	DeSimone et al.	370/260
6,052,725 A	4/2000	McCann et al.	709/223
6,058,431 A *	5/2000	Srisuresh et al.	709/245
6,061,349 A	5/2000	Coile et al.	370/389
6,118,768 A	9/2000	Bhatia et al.	370/254
6,128,657 A	10/2000	Okanoya et al.	709/224
6,393,017 B1	5/2002	Galvin et al.	370/352
6,614,774 B1	9/2003	Wang	370/338
6,738,382 B1	5/2004	West et al.	370/401
6,850,497 B1 *	2/2005	Sigler et al.	370/310

FOREIGN PATENT DOCUMENTS

(21) Appl. No.: **10/746,275**

EP 1 017208 A2 7/2000

(22) Filed: **Dec. 23, 2003**

OTHER PUBLICATIONS

K. Egevang, et al., "The IP Network Address Translator
(NAT)," May 1994, RFC 1631.

* cited by examiner

(65) **Prior Publication Data**

US 2005/0041602 A1 Feb. 24, 2005

Primary Examiner—Ajit Patel

(74) *Attorney, Agent, or Firm*—Beyer Weaver & Thomas,
LLP

Related U.S. Application Data

(62) Division of application No. 09/256,719, filed on Feb.
24, 1999, now Pat. No. 6,738,382.

(57) **ABSTRACT**

Methods and apparatus are described for providing access to
a network via a first one of a plurality of network access
nodes in the network. The network access nodes each have
a network address associated therewith which is unique on
the network, the first network access node having a first
network address associated therewith. The first network
address is associated with a first computer while the first
computer is connected to the first network access node
thereby providing access to the network.

(51) **Int. Cl.**

H04L 12/16 (2006.01)

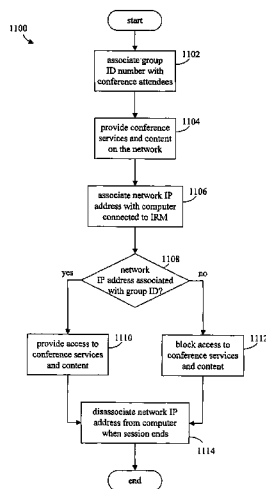
H04Q 11/00 (2006.01)

(52) **U.S. Cl.** **370/260; 379/202.01**

(58) **Field of Classification Search** 370/389,
370/259, 260, 261, 392, 390, 401, 432, 475;
379/201.01, 202.01; 455/414, 415, 416

See application file for complete search history.

15 Claims, 12 Drawing Sheets



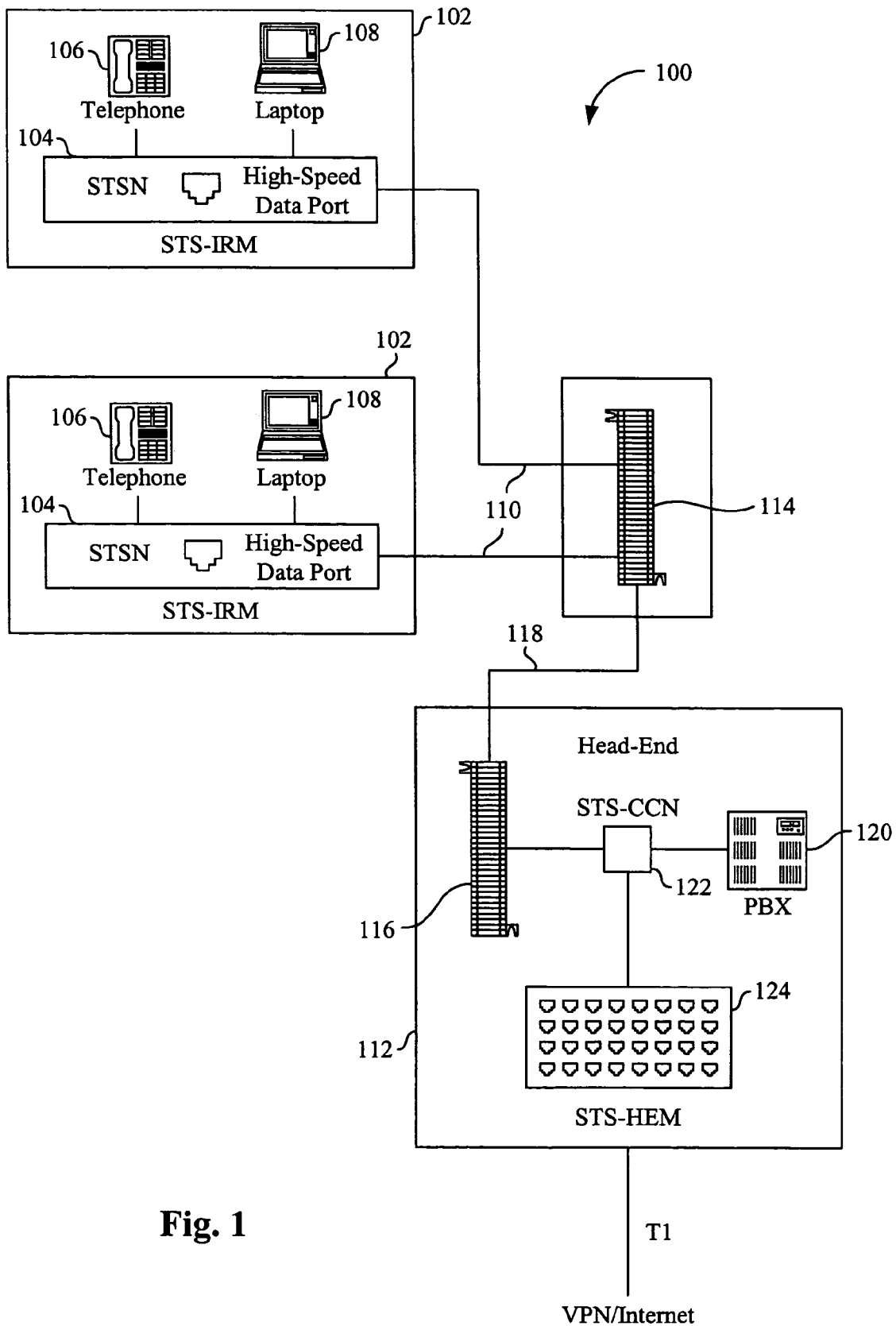


Fig. 1

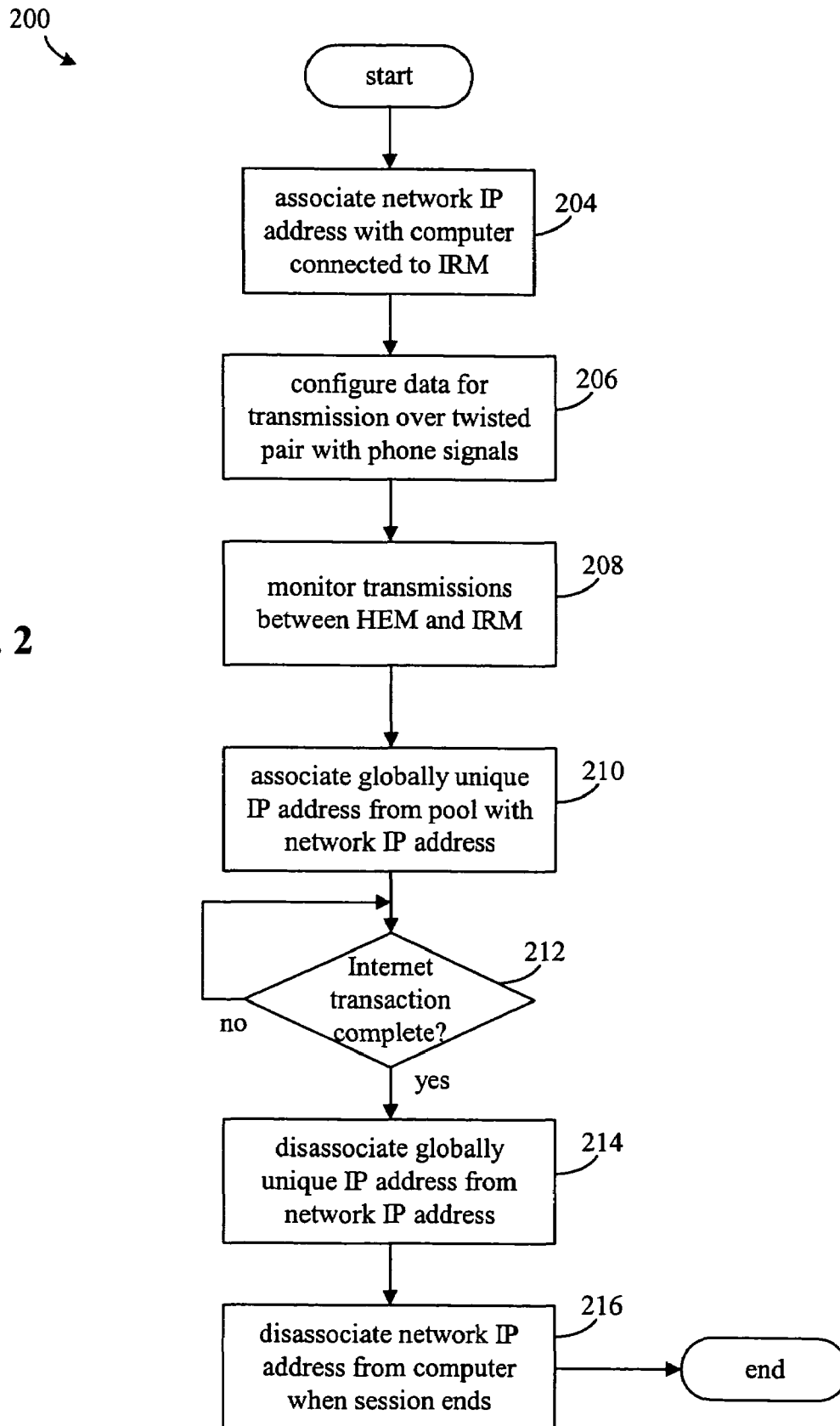
U.S. Patent

Feb. 7, 2006

Sheet 2 of 12

US 6,996,073 B2

Fig. 2



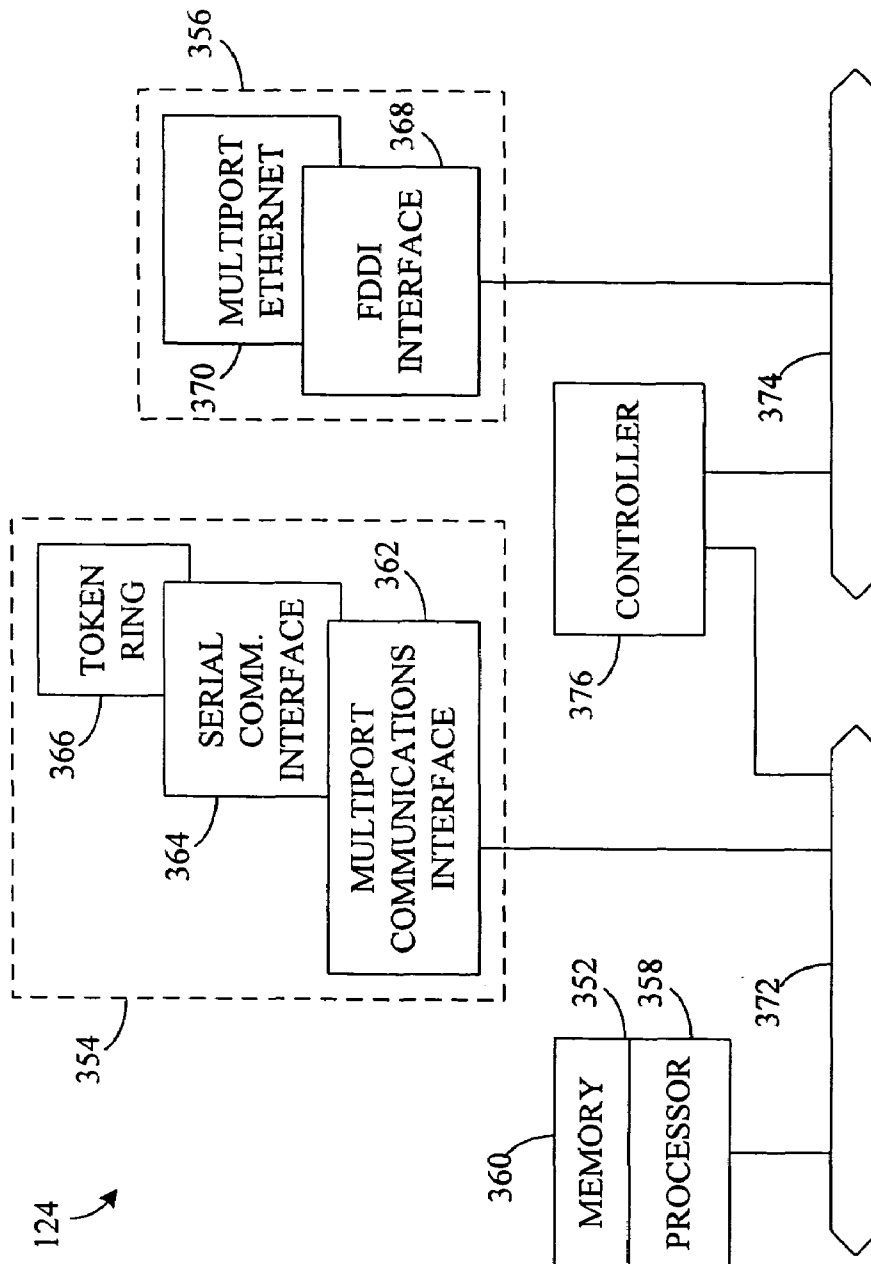


Fig. 3b

U.S. Patent

Feb. 7, 2006

Sheet 5 of 12

US 6,996,073 B2

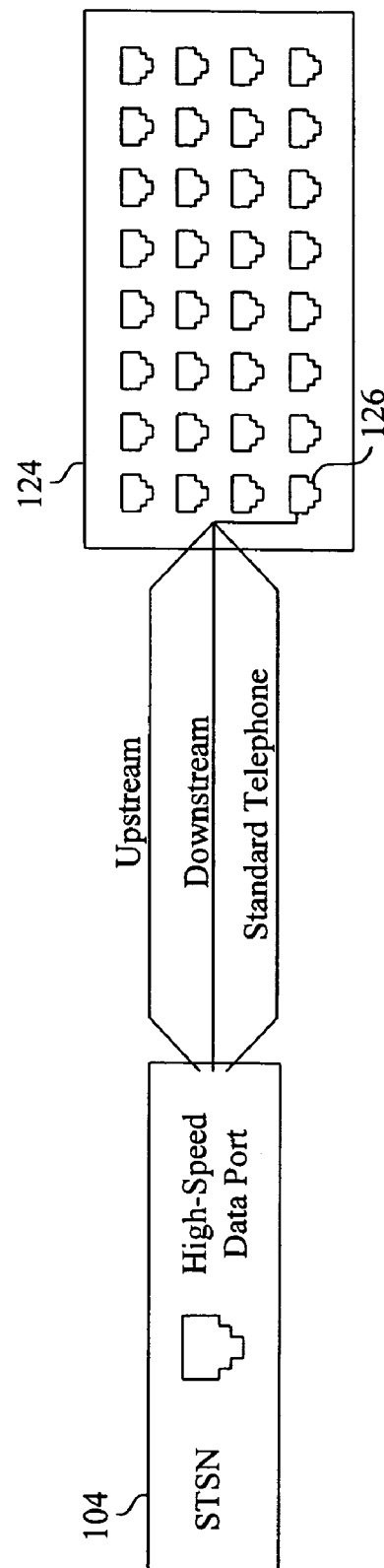


Fig. 4

U.S. Patent

Feb. 7, 2006

Sheet 6 of 12

US 6,996,073 B2

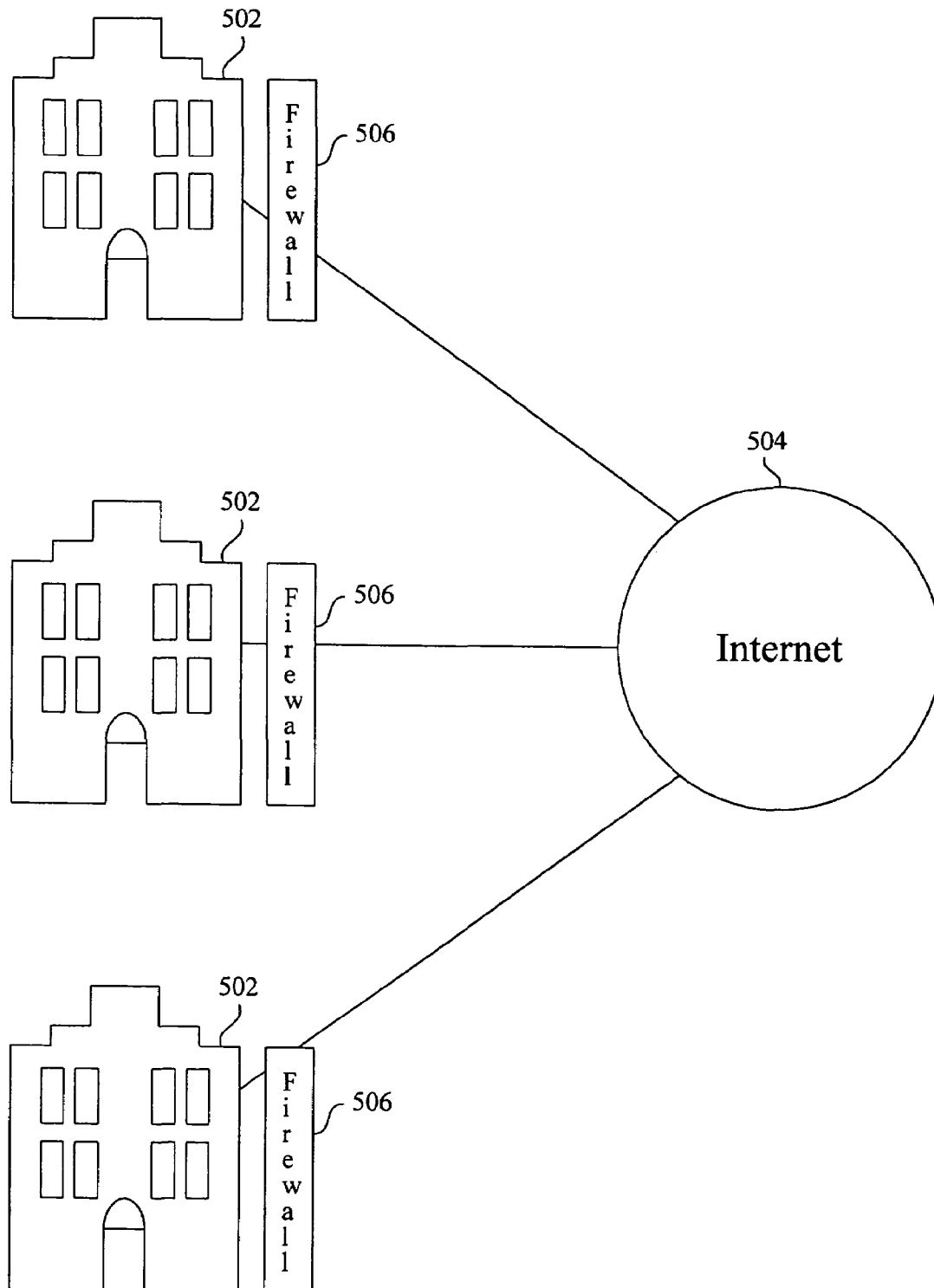


Fig. 5

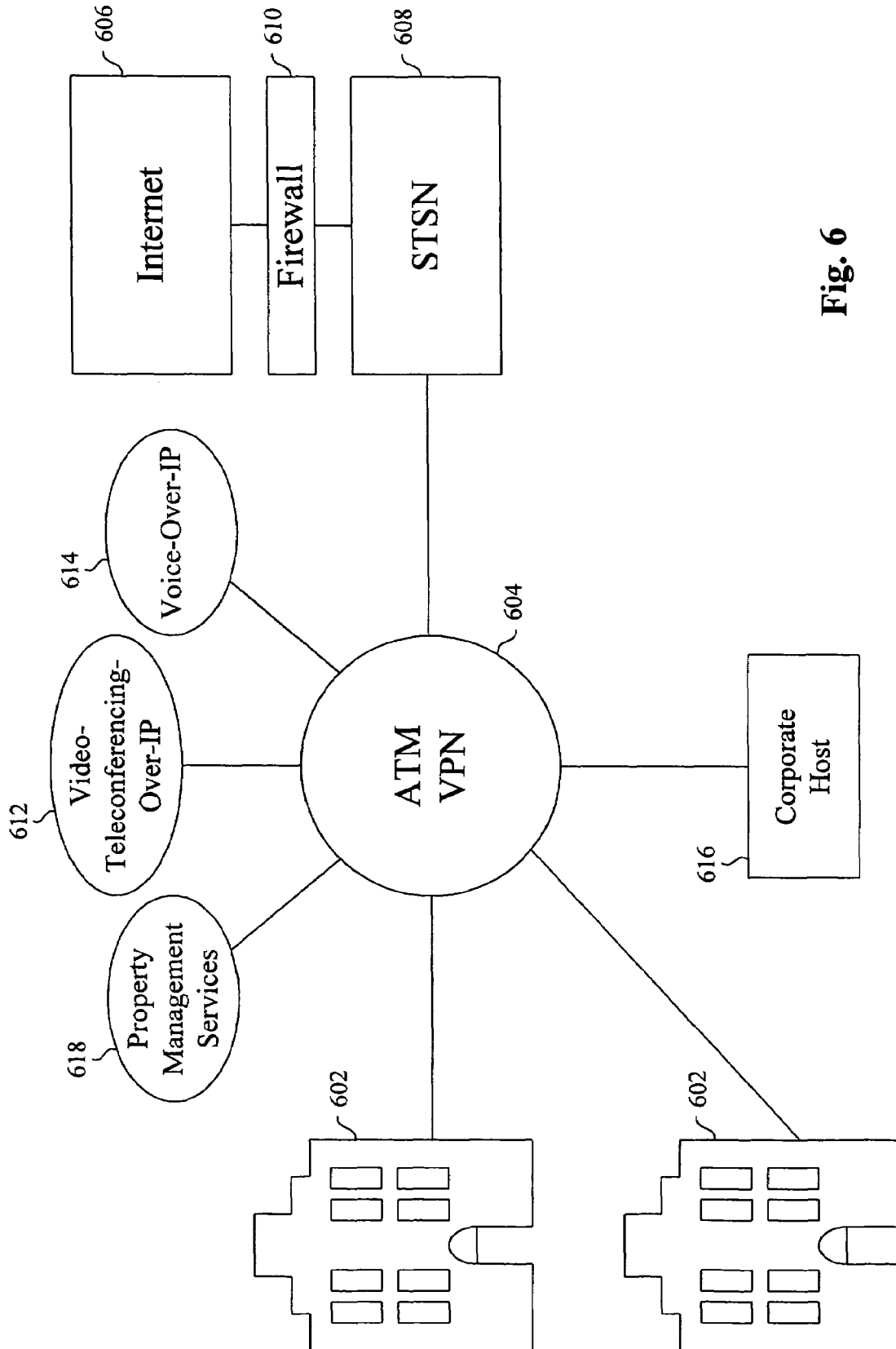


Fig. 6

U.S. Patent

Feb. 7, 2006

Sheet 8 of 12

US 6,996,073 B2

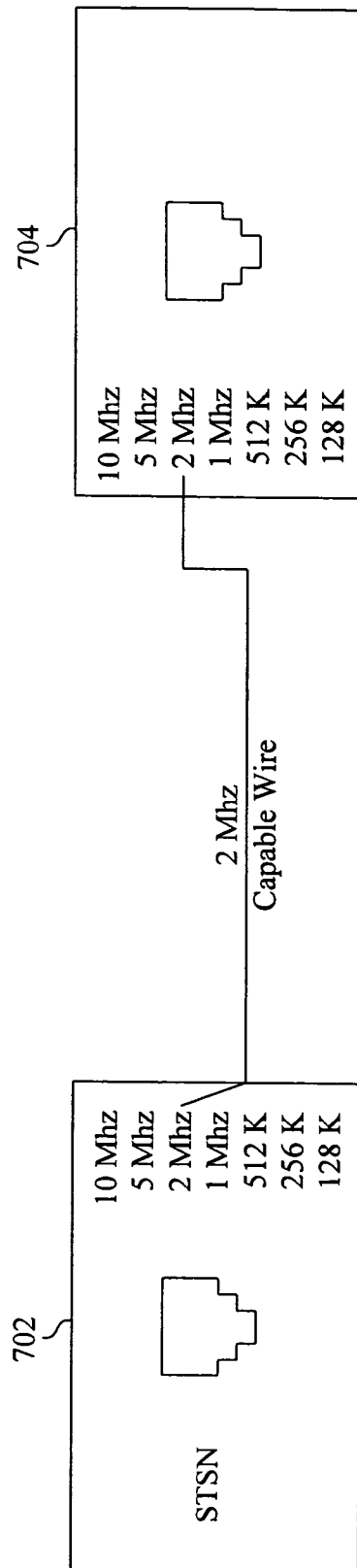
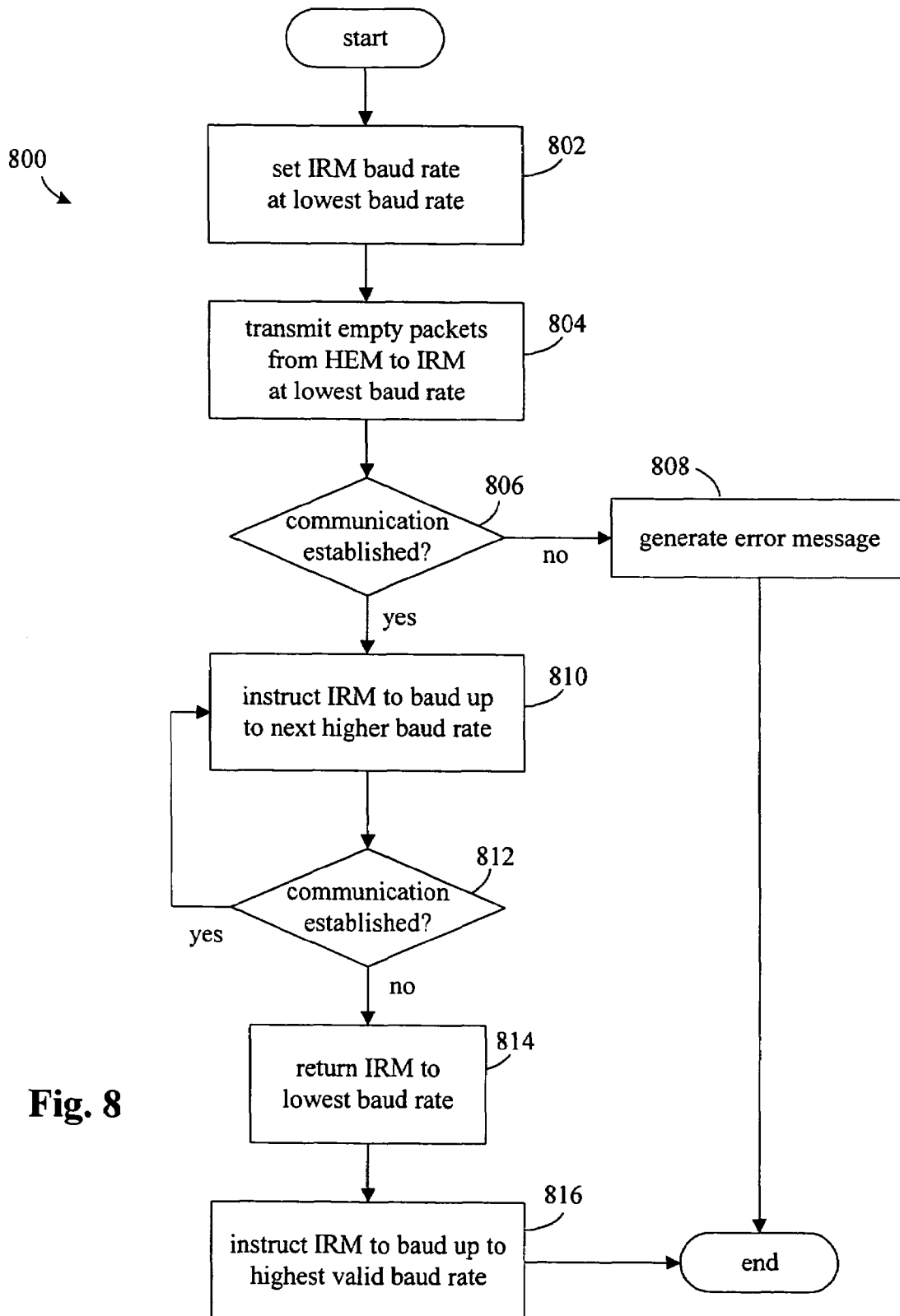


Fig. 7



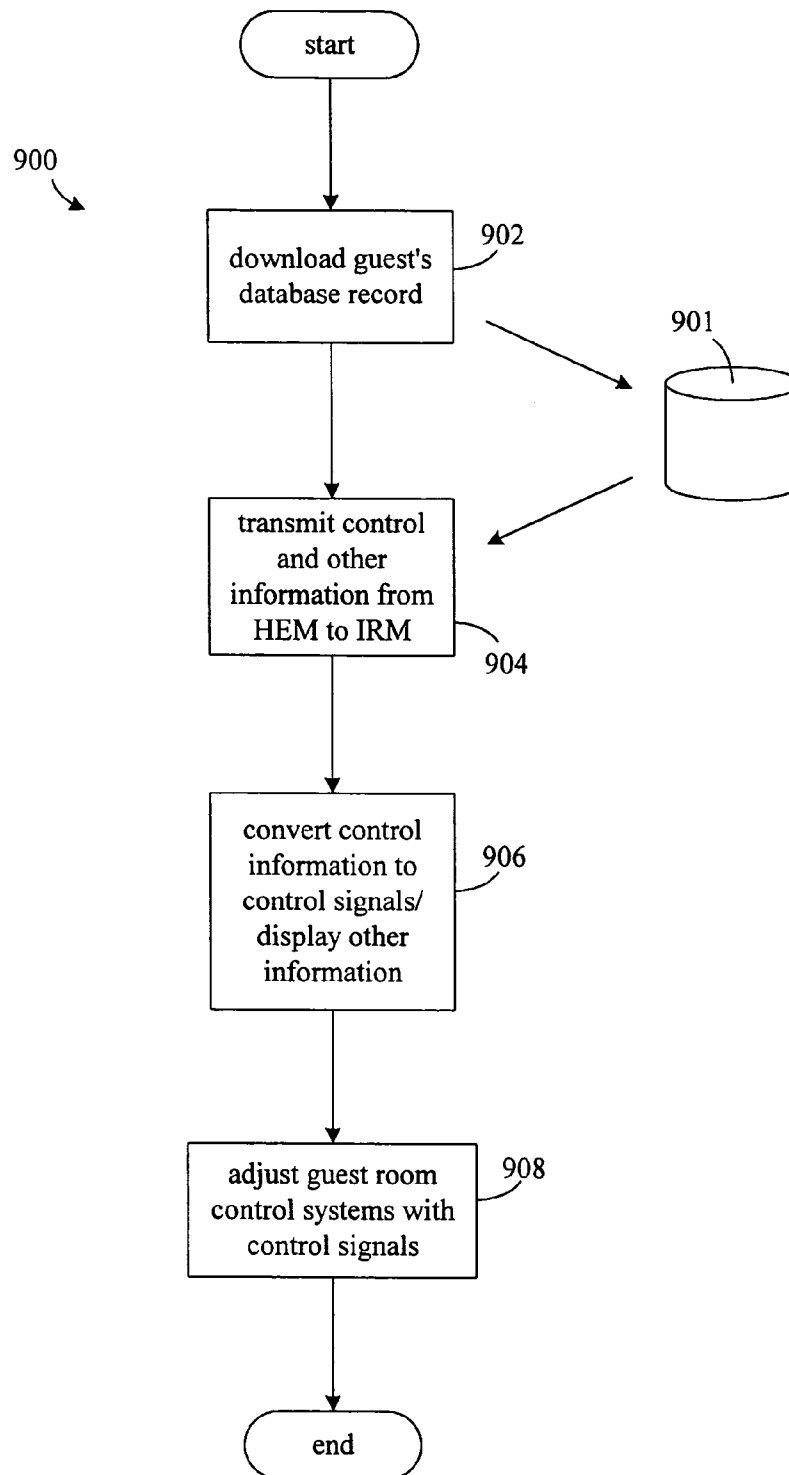


Fig. 9

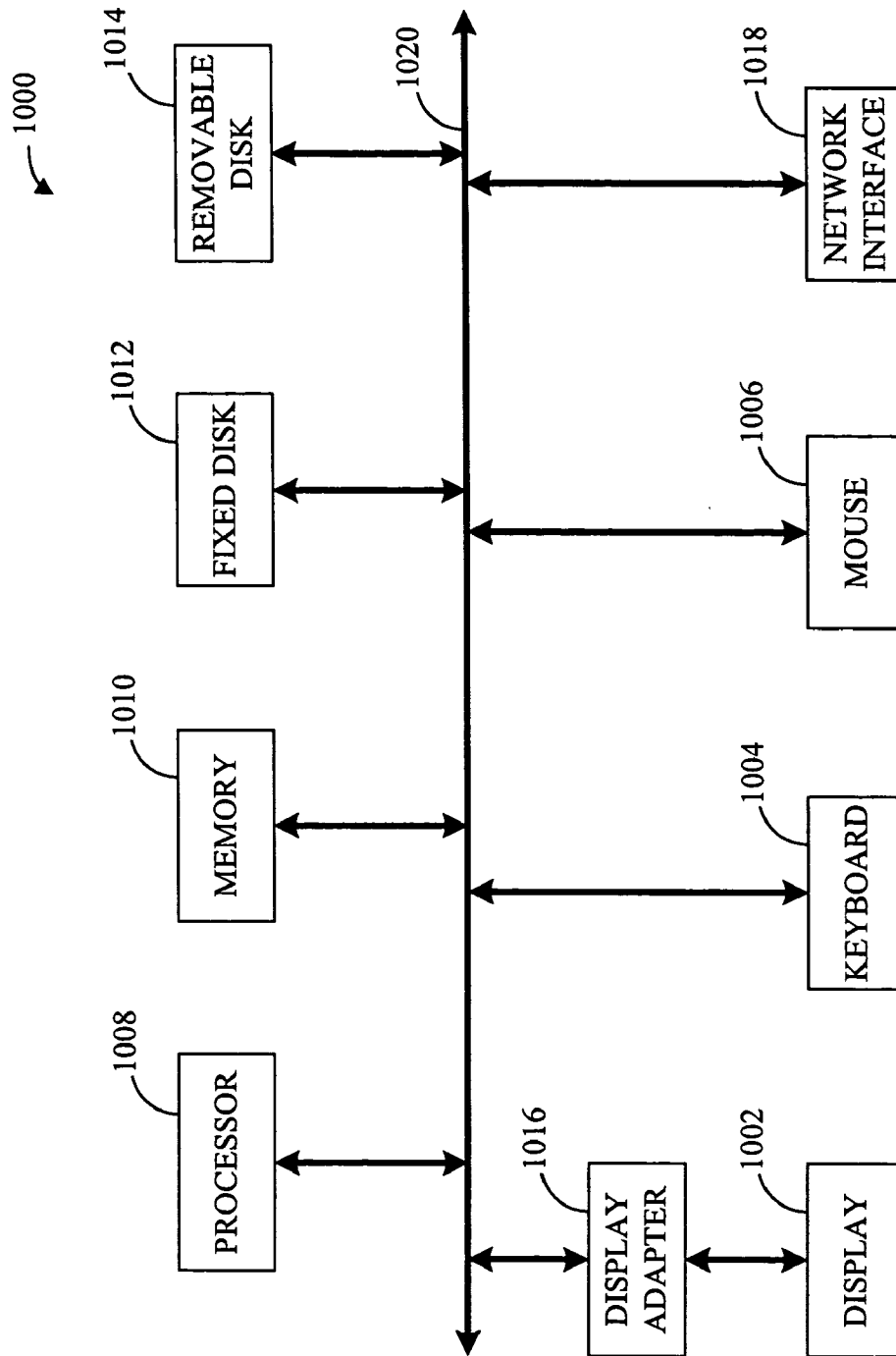
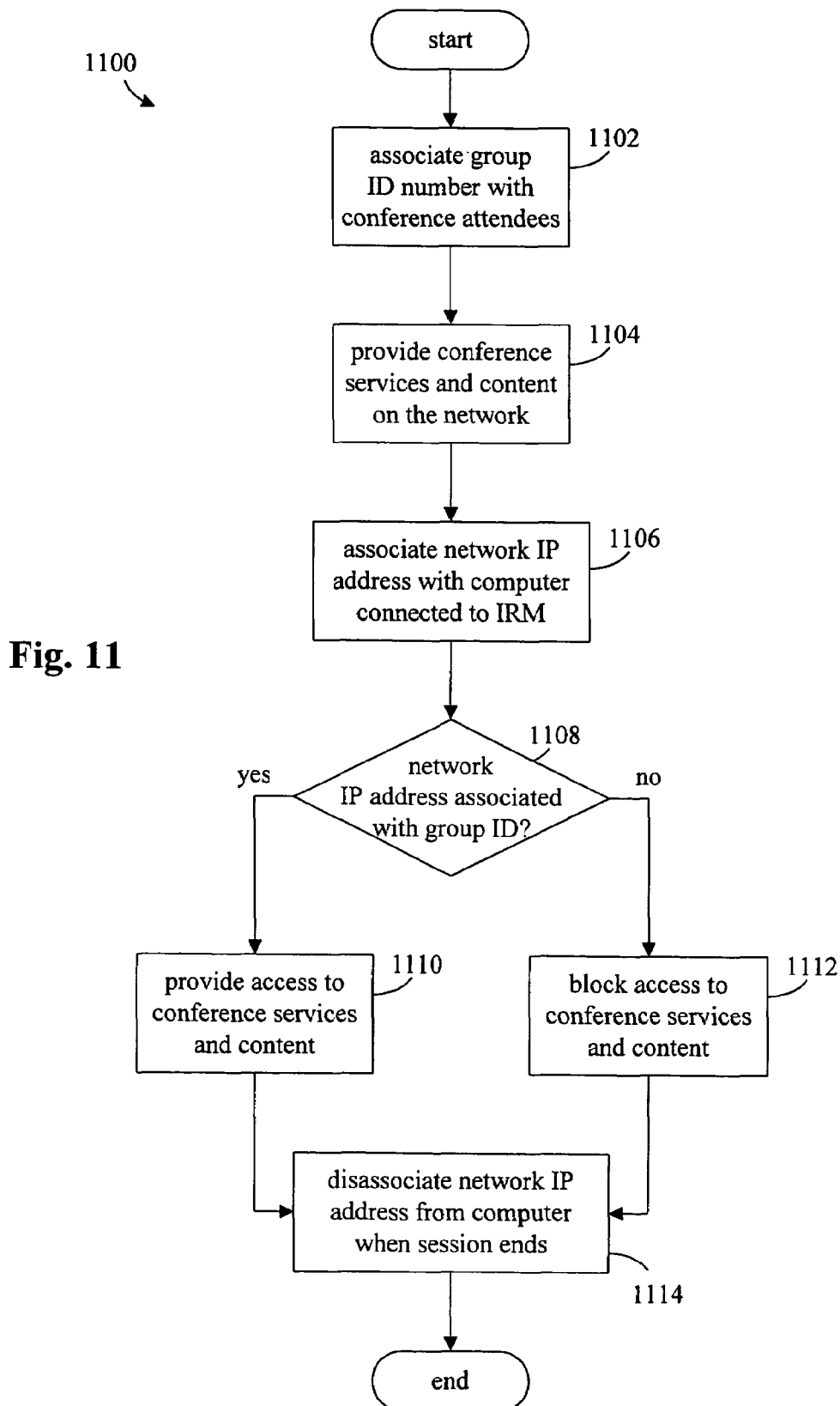


Fig. 10



US 6,996,073 B2

1

METHODS AND APPARATUS FOR PROVIDING HIGH SPEED CONNECTIVITY TO A HOTEL ENVIRONMENT

RELATED APPLICATION DATA

The present application is a divisional of and claims priority from U.S. patent application Ser. No. 09/256,719 filed Feb. 24, 1999 now U.S. Pat. No. 6,738,382, the entire disclosure of which is incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

The present invention relates to network communications and, more specifically, to providing high speed Internet access to users in hotel environments.

Any business traveler who relies on network communications to maintain contact with clients and the home office appreciates the availability of fast and reliable data ports at remote locations such as airport lounges and hotel rooms. The hospitality industry has only recently begun to understand the necessity of providing such high speed data connections to business travelers. In fact, given the explosive growth of network technologies and the corresponding dependence of the business professional on such technologies, hotels which do not move to provide high speed connectivity in guest rooms comparable to the typical office environment will likely lose a substantial portion of their business to hotels which do.

Unfortunately, many hotel rooms are not currently wired to accommodate high speed data traffic. That is, prior to 1990, virtually all hotel rooms were wired to provide only basic telephone service. As late as 1995, less than 10% of hotel rooms were wired to handle standard Ethernet data speeds. Even today, while the major players in the hospitality industry are searching for high speed connectivity solutions, the vast majority of hotel guest and conference rooms are still wired with low quality, single pair connections. One obvious solution would be to completely rewire all of the guest and conference rooms in each hotel facility to provide the desired data transmission capabilities. However, given the prohibitive cost of such an undertaking, a less costly solution would be desirable.

Even if such a costly rewiring were undertaken, there are other problems which are not addressed by an infrastructure upgrade. For example, even if a high speed connection to the hotel's host is provided, it will often be the case that a guest's laptop computer would be incompatible with the hotel network in some way. Thus, each guest's laptop must be configured appropriately in order to communicate with the network and with the Internet beyond. This would likely involve loading special software onto a guest's laptop each time the guest wants to go online. Not only would such a process be cumbersome and annoying to the hotel guest, it may also be unacceptable from the guest's point of view in that reconfiguring the laptop may interfere with the current configuration in undesirable ways.

Neither does a costly wiring upgrade address the administrative and security issues related to providing Internet access via a hotel host. That is, high speed Internet access for hotel guests requires a network at the hotel property and some sort of connection between the hotel network and the Internet, e.g., a T1 or T3 line. A firewall at each hotel property would also be required to protect the internal network from unauthorized access. The existence of the firewall at each property, in turn, requires that most of the

2

control and administration of the local network be performed at the hotel property rather than remotely, thus representing an undesirable redundancy of administrative functions.

Another administrative difficulty related to maintaining each hotel property as a separate Internet host involves the management of IP addresses. Ranges of globally unique 32-bit IP addresses are issued to organizations by a central Internet authority. These addresses are organized in a four octet format. Class A IP addresses are issued to very large organizations and employ the first of the four octets to identify the organization's network and the other three to identify individual hosts on that network. Thus, a class A address pool contains nearly 17 million (2^{24}) globally unique IP addresses. With class B addresses, the first two octets are used to identify the network and the last two to identify the individual hosts resulting in 64,000 (2^{16}) globally unique IP addresses for each organization. Finally, with class C addresses, the first three octets are used to identify the network and the last octet to identify the individual hosts resulting in only 256 (2^8) globally unique IP addresses for each organization.

Unfortunately for many medium to large size organizations (1,000 to 10,000 hosts), it has become very difficult, if not impossible, to obtain anything other than a class C address for their networks due to the fact that the class A and B address spaces have been almost entirely locked up. This problem has been addressed to some extent by the use of a Network Address Translation (NAT) protocol. According to such a protocol, when a local host on an organization's network requests access to the Internet, it is assigned a temporary IP address from the pool of globally unique IP addresses available to the organization. The local host is identified by the globally unique address only when sending or receiving packets on the Internet. As soon as the local host disconnects from the Internet, the address is returned to the pool for use by any of the other hosts on the network. For additional details on the implementation of such a protocol please refer to K. Evegang and P. Francis, *The IP Network Address Translator (NAT), Request for Comments "RFC" 1631*, Cray Communications, NTT, May 1994, the entirety of which is incorporated herein by reference for all purposes.

Such dynamic assignment of IP addresses might be sufficient for certain organizations as long as the number of simultaneous users which require access to the Internet remains below the maximum of 256. However, if, for example, a 1200 room hotel were hosting an Internet technologies seminar it would be extremely likely that the demand for Internet access would exceed the available address pool. All of this also assumes that a major hotel chain would be able to obtain a complete class C pool of addresses for each of its properties; not necessarily a reasonable assumption.

It is therefore desirable to provide methods and apparatus by which each of the properties in a major hotel chain may provide high speed Internet access to each of its guest rooms in a secure, inexpensive, and reliable manner without undue administrative burdens on the individual properties.

SUMMARY OF THE INVENTION

According to the present invention, methods and apparatus are provided which make use of existing hotel wiring infrastructures to provide secure, high speed data and Internet access to each of the guest rooms in a hotel property. Specific implementations of the technology described herein have the ability to auto-baud down to whatever speed the

US 6,996,073 B2

3

wiring infrastructure will allow thus providing the maximum bandwidth allowable by that infrastructure. According to specific embodiments, the present invention is able to select the maximum baud rate appropriate for each individual guest room. According to other specific embodiments, where the wiring to the guest rooms is a single pair phone line, the present invention allows 1 Megabit half duplex data transmissions to coexist on the single pair with standard telephone signals.

According to one embodiment of the invention, each guest room in the hotel is interconnected via the hotel's current wiring infrastructure into a local network. When a guest wishes to access the Internet, he connects his laptop to an in-room module installed in each guest room which temporarily assigns a "fake" local IP address to the guest's laptop. The "fake" local IP address is associated with the in-room module and is unique on the hotel's local network. The address is "fake" in that it is not a valid Internet address and in that it replaces the laptop's own real IP address. The assigned local IP address uniquely identifies the guest's laptop on the hotel network while that laptop remains connected to the in-room module.

A headend module in the hotel handles packet routing and provides access to the Internet. In facilitating access to the Internet, the headend module temporarily assigns globally unique IP addresses from a pool of, for example, class C addresses to in-room modules in individual guest rooms in response to requests for Internet access from those rooms. An assigned IP address remains dedicated to a particular in-room module (and thus the associated guest's computer) for the duration of the Internet transaction. Upon termination of the transaction, the globally unique IP address is disassociated from the in-room module and put back into the pool for use in facilitating a later Internet transaction from any of the hotel's rooms.

According to another embodiment of the invention, the local networks of a number of hotels are interconnected via a remote server thereby forming a private wide area network, or a virtual private network. The operation of the virtual private network to provide high speed data and Internet access to individual guest rooms is similar to the process described above except that the "fake" IP address of the in-room modules are unique over the entire virtual private network, and the temporary assignment of globally unique IP addresses is performed by the remote server rather than the hotel headend. This is advantageous in that it is contemplated that the remote server has a larger pool of such addresses associated therewith than an individual hotel network might be able to procure (e.g., a class B address pool).

Thus, because the IP address needs of all of the hotels in the virtual private network are spread out over the entire installed base of the remote server, bursts of need at any one property which exceed the capacity of a single class C address pool may be accommodated. The virtual private network embodiment of the present invention also has the advantage that firewall security and other network administrative functions may be centralized and performed remotely without compromising the security of any individual hotel network.

Thus, according to the present invention, methods and apparatus are provided for providing access to a network via a first one of a plurality of network access nodes in the network. The network access nodes each have a network address associated therewith which is unique on the network, the first network access node having a first network address associated therewith. The first network address is

4

associated with a first computer while the first computer is connected to the first network access node thereby providing access to the network.

According to a more specific embodiment, Internet access is provided to a first computer via a first one of a plurality of network access nodes in a network using a plurality of globally unique IP addresses. The network access nodes each have a network address associated therewith which is unique on the network, the first network access node having a first network address associated therewith. The first network address is associated with the first computer while the first computer is connected to the first network access node thereby providing access to the network. A first one of the globally unique IP addresses is associated with the first network address for conducting an Internet transaction. The first globally unique IP address is disassociated from the first network address upon termination of the Internet transaction. The first globally unique IP address is then available for association with any of the network addresses. According to one embodiment, the network comprises a local area network and the associating and disassociating of the globally unique IP address is done by a headend associated with the local area network. According to another embodiment, the network comprises a wide area network and the associating and disassociating of the globally unique IP address is done by a remote server which controls the wide area network.

According to a specific embodiment, a network is provided having a plurality of network access nodes each having a network address associated therewith which is unique on the network. Each network access node is for providing access to the network for a computer connected to the network access node. A headend module interconnects the network access nodes. The network address associated with each network access node is associated with the computer connected thereto thereby providing access to the network.

According to another specific embodiment, a wide area network is provided having a plurality of networks each comprising a plurality of network access nodes. Each network access node has a network address associated therewith which is unique among the plurality of networks. Each network access node provides access to the wide area network for a computer connected to the network access node. A remote server interconnects the plurality of networks into the wide area network. The network address associated with each network access node is associated with the computer connected thereto thereby providing access to the wide area network.

According to yet another specific embodiment, a network access node is provided for providing access to a network of which the network access node is a part. The network access node has a network address associated therewith which is unique on the network. According to a more specific embodiment, the network address node is operable to associate the network address with a computer while the computer is connected to the network access node thereby providing access to the network.

According to a further specific embodiment, a headend module is provided for interconnecting a plurality of network access nodes in a network. Each network access node has a network address associated therewith which is unique on the network and provides access to the network for a computer connected to the network access node. According to a more specific embodiment, the headend module associates the network address associated with each network access node with the computer connected thereto thereby providing access to the network.

US 6,996,073 B2

5

According to another specific embodiment, methods and apparatus are provided for providing conference services over a network having a plurality of users associated therewith. A group identification tag is associated with selected ones of the plurality of users thereby identifying the selected users as attendees of the conference. The conference services are provided on the network. Access to the conference services is then restricted to the selected users using the group identification tag.

A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a hotel according to a specific embodiment of the invention;

FIG. 2 is a flowchart illustrating a method for providing high speed data and Internet access to guest rooms in a hotel according to a specific embodiment of the invention;

FIGS. 3a and 3b are more detailed block diagrams of the in-room module and head-end module of FIG. 1;

FIG. 4 is a block diagram illustrating the combination of half duplex data and standard telephone data on a single pair of conductors according to a specific embodiment of the invention;

FIG. 5 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in hotels according to another specific embodiment of the invention;

FIG. 6 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in hotels according to yet another specific embodiment of the invention;

FIG. 7 is a block diagram illustrating the auto-bauding technique of the present invention;

FIG. 8 is a flowchart illustrating the auto-bauding technique of the present invention;

FIG. 9 is a flowchart illustrating the customization of a guest room and the transmission of control information to in-room systems via a hotel network;

FIG. 10 is a block diagram of file server for use with various embodiments of the present invention; and

FIG. 11 is a flowchart illustrating the providing of online conference services.

DESCRIPTION OF SPECIFIC EMBODIMENTS

FIG. 1 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a hotel according to a specific embodiment of the invention. In each guest room 102 is an in-room module (IRM) 104 by which a telephone 106 and a guest's laptop computer 108 may be connected to the hotel's wiring infrastructure. According to a specific embodiment, IRM 104 is plugged directly into the room's phone jack and has at least two additional ports, one for the room's telephone, e.g., an RJ-11 jack, and one for the guest's laptop, e.g., an RJ-45 Ethernet port. According to various embodiments, IRM 104 performs a number of functions including, for example, combining and separating Ethernet data and standard telephone signals for transmission over the hotel's wiring infrastructure. According to other embodiments and as discussed below, IRM 104 is configured to receive control information from a central location for automated control of various room environmental parameters, e.g., temperature and lighting. According to still other embodiments, IRM 104

6

is configured to receive a wide variety of other types of data such as, for example, digital audio and video for presentation in the guest room, or a wide variety of other information services.

Transmission line 110 connects IRM 104 to the hotel's head-end 112 via any of a wide variety of infrastructures. In the example shown, transmission line 110 connects IRM 104 to head-end 112 via standard telephone company wiring as represented by punch down blocks 114 and 116 and telephone company transmission line 118. It will be understood, however, that the wiring between IRM 104 and head-end 112 may take other forms such as, for example, a four-conductor Ethernet network. Head-end 112 comprises punch down block 116 and public branch exchange (PBX) 120. Interposed between punch down block 116 and PBX 120 is a connection port 122 which, according to a specific embodiment, may be easily installed simply by unplugging the standard 24-pin connector from PBX 120, plugging connection port 122 into the PBX connector (not shown), and plugging the original connector from punch down block 116 into connection port 122. Standard telephone signals pass through connection port 122 to PBX 120 while half duplex Ethernet data packets are transmitted and received by head-end module (HEM) 124.

Depending on the configuration of the present invention, HEM 124 performs a variety of functions and, according to some embodiments, can be thought of as an enhanced router with additional capabilities programmed into its operating system. That is, according to such embodiments, HEM 124 serves as a switch which routes data packets to and from IRMs 104, and serves as the other end of the communications to and from IRMs 104 in which Ethernet data and phone signals are combined over single twisted pair technology. According to other alternative embodiments, HEM 124 handles address translation and assignment, controls network access, and serves as a bridge for Ethernet data transmitted over the hotel's single twisted pair infrastructure. HEM 124 has a plurality of ports 126 each of which communicates with a corresponding IRM 104. This communication may be individually monitored and controlled (by either the IRM or the HEM) thus allowing central hotel management of billing and access as well as the ability to generate reports for troubleshooting purposes.

Each IRM 104 (and thus the corresponding HEM port 126) has a fixed IP address which may be configured using the Simple Network Management Protocol (SNMP). If the guest's computer connected to a particular IRM 104 does not have its own internal IP address, the fixed IP address of the corresponding IRM 104/HEM port 126 is assigned to the guest's computer using the Dynamic Host Configuration Protocol (DHCP) to facilitate access to network 100. If the guest's computer already has its own internal IP address, address translation is performed between the computer's internal IP address and the fixed IP address of the IRM 104/HEM port 126. According to various embodiment of the invention, this address translation may be performed by either IRM 104 or HEM 124. HEM 124 has a small boot ROM (not shown) for basic IP communications and a large flash ROM (not shown) for fully functional software and configuration data. This allows for remote software upgrades using, for example, an encrypted protocol riding on top of IP.

FIG. 2 is a flowchart 200 illustrating a method for providing high speed data and Internet access to guest rooms in a hotel using the system of FIG. 1. When a guest's computer connects to an IRM in any one of the guest rooms, the network IP address associated with that IRM is associ-

US 6,996,073 B2

7

ated with the computer (204). As discussed above, this association could mean a DHCP assignment of the network IP address to the guest's computer where the computer did not already have an internal IP address. It could also mean that the internal IP address of the computer is translated into the network IP address. This address assignment/translation may be effected by either the IRM and the HEM. In addition, it will be understood that depending on where the assignment/translation occurs it may precede or follow 206 described below. The network IP address is associated with the guest's computer while it remains connected to the IRM.

Where the transmission line connecting the IRM to the hotel network comprises a single twisted pair of conductors, the data communications between the IRM and the HEM are configured so that they may be transmitted substantially simultaneously over the single twisted pair with the standard telephone signals from the phone in the guest room (206). A specific technique by which this configuration is effected is described below with reference to FIGS. 3a and 4.

Once the connection is established, the communications between the IRM and the HEM are monitored either periodically or continuously for a variety of purposes (208). This information may be used by the hotel for billing purposes or for troubleshooting and improving the reliability of the hotel network.

If an Internet transaction is requested by the guest's computer, a globally unique IP address from a pool of such addresses is temporarily associated with the network IP address currently associated with the guest's computer using, for example, a network address translation protocol (210). As discussed above, the pool of addresses could be, for example, class A, B, or C addresses. As will be discussed below with reference to FIGS. 5 and 6, the temporary association of the globally unique IP address may be done by the HEM in the hotel or, according to another embodiment, by a remote server which interconnects one or more hotel properties in a wide area network. When the Internet transaction is complete (212), the globally unique IP address is disassociated from the network IP address and put back in the pool for use in facilitating subsequent Internet transactions from any of the hotel's guest rooms (214). The network IP address remains associated with the guest's computer until the session ends, e.g., the computer is disconnected from the IRM or powered down (216).

FIGS. 3a and 3b are more detailed block diagrams of IRM 104 and HEM 124 of FIG. 1, respectively. IRM 104 comprises connection circuitry for connecting the IRM to the room's standard telephone jack as well as the room's telephone and the guest's computer. According to a specific embodiment, the connection circuitry includes RJ-11 ports 302 for connecting to the phone and 303 for connecting to the wall jack, an Ethernet port 304, an IEEE 1394 port 305, and a universal serial bus (USB) port 306 for connecting to the guest's computer, and an additional data port 307 for receiving various types of data. IEEE 1394 port 305 and USB port 306 may, in some instances, prove more convenient than Ethernet port 304 in that certain network reconfiguration issues don't have to be dealt with. In addition, many business travelers often don't travel with the Ethernet dongle which is necessary for connecting their laptop's Ethernet port to a network Ethernet port. Thus, depending upon which of the two alternate standards, IEEE 1394 or USB, the laptop is configured for, IRM 104 is operable to translate the laptop's transmissions to the Ethernet standard.

According to a specific embodiment, IRM 104 also includes transmission circuitry 308 for transmitting and receiving data on a single twisted pair of conductors of

8

which the majority of hotel wiring infrastructures are comprised. According to one embodiment, a portion of transmission circuitry 308 is implemented according to the home PNA (Phone-line Networking Alliance) standard which allows half duplex data and phone signals on the same line as illustrated by the diagram of FIG. 4. According to the home PNA standard, data transmissions from IRM 104 to a port 126 of HEM 124 and transmissions from the HEM to the IRM are alternated at a frequency in the range of 4–9 MHz. Because standard phone signals exist at a relatively low frequency compared to the home PNA modulation frequency, all of the signals may easily exist on a single pair of wires.

According to a specific embodiment, transmission circuitry 308 is operable to associate the network IP address associated with IRM 104 with the guest's computer. That is, the address translation or assignment which allows the guest access to the local or wide area network is performed by the transmission circuitry in the IRM. According to a more specific embodiment, transmission circuitry 308 includes a processing unit 309 based on RISC microprocessor which performs the address translation, the combining and separation of signals for transmission to the headend, and the routing of the received signals to the appropriate IRM port. According to a specific embodiment, processing unit 309 comprises an Intel 80960VH and the appropriate support circuitry.

According to another specific embodiment, IRM 104 also includes control circuitry 310 for receiving control information via the hotel's network for controlling one or more control systems 311 proximate to the IRM. As will be discussed below with reference to FIG. 9, such control systems may include, for example, the room's temperature control, lighting, and audio systems. In one embodiment, the control circuitry includes conversion circuitry 312 for converting the received control information into the necessary control signals for actually controlling the in-room control systems. The conversion circuitry may include, for example, an RF transmission element 314 (e.g., an antenna) for transmitting RF control signals to the various control systems. According to an alternative embodiment, conversion circuitry 312 includes an infrared transmission element (e.g., an IR diode) for transmitting infrared control signals to various control systems.

Transmission circuitry 308 (using processor 309) discriminates between the various data it receives and directs it to the appropriate port on IRM 104 according to address information in data packet headers. According to a specific embodiment, digital audio and video may be transmitted to individual rooms via the system described herein. The digital audio and video are directed to additional data port 307 to which an audio and/or video system may be connected for presenting the transmitted content. In this way, an ambience may be set for the guest's arrival. In addition, the guest could select a wide variety of entertainment and information services via the hotel network which may then be transmitted to the guest's room via the auxiliary data port 307 on IRM 104. According to one embodiment, data port 307 receives audio data which directly drives a pair of speakers in the guest room.

Specific embodiments of IRM 104 also include an LED or LCD display 316 on which status and other information may be communicated to the occupant of the guest room whether or not they are currently connected. For example, before a connection is made, display 316 could be used to inform the hotel guest of all of the services available through IRM 104 as well as instructions for connecting to IRM 104. Other

US 6,996,073 B2

9

information such as stock quotes and weather information may also be presented continuously or periodically. Once connected, display **316** could communicate the status of the connection as well as the time connected and current connection charges. It will be understood that a wide variety of other information may be presented via display **316**.

IRM **104** may also include an array of individual colored LEDs **318** which provide information to the user. Such LEDs may indicate, for example, the connection status of the IRM, i.e., whether it is connected to the HEM, using red or green LEDs. LEDs **318** may also be configured to indicate a purchase status to the user. That is, because connection services are often purchased in 24 hour blocks, LEDs **318** may indicate to the user whether she is operating within a block of time which has already been paid for (green), whether the end of the current block is approaching (yellow), or whether she has already entered the next time block (red). LEDs **318** could also indicate which type of connection the user has established, e.g., USB, Ethernet, or IEEE 1394.

As mentioned above and as shown in FIG. **3b**, HEM **124** may be thought of as an enhanced router which routes data packets to and from IRMs **104**, controls network access, serves as a bridge for Ethernet data transmitted over the hotel's single twisted pair infrastructure, and, according to some embodiments, handles address translation and assignment. According to one embodiment, a 2611 router from Cisco Systems, Inc. is used to implement HEM **124**. HEM **124** includes a master central processing unit (CPU) **352**, low and medium speed interfaces **354**, and high-speed interfaces **356**. When acting under the control of appropriate software or firmware, the CPU **352** is responsible for such router tasks as routing table computations and network management. It may also be responsible for controlling network access and transmissions, etc. It preferably accomplishes all these functions under the control of software including an operating system (e.g., the Internet Operating System (IOS®) of Cisco Systems, Inc.) and any appropriate applications software. CPU **352** may include one or more microprocessor chips **358**. In a specific embodiment, a memory **360** (such as non-volatile RAM and/or ROM) also forms part of CPU **352**. However, there are many different ways in which memory could be coupled to the system.

The interfaces **354** and **356** are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receipt of data packets over the network and sometimes support other peripherals used with HEM **124**. The low and medium speed interfaces **354** include a multiport communications interface **362**, a serial communications interface **364**, and a token ring interface **366**. The high-speed interfaces **356** include an FDDI interface **368** and a multiport Ethernet interface **370**. Preferably, each of these interfaces (low/medium and high-speed) includes (1) ports for communication with the appropriate media, (2) an independent processor, and in some instances (3) volatile RAM. The independent processors control such communications intensive tasks as packet switching, media control and management. By providing separate processors for the communications intensive tasks, this architecture permits the master microprocessor **352** to efficiently perform routing computations, network diagnostics, security functions, etc.

The low and medium speed interfaces **354** are coupled to the master CPU **352** through a data, control, and address bus **372**. High-speed interfaces **356** are connected to the bus **372** through a fast data, control, and address bus **374** which is in turn connected to a bus controller **376**.

10

Although the system shown in FIG. **3b** is one type of router by which the present invention may be implemented, it is by no means the only router architecture by which the present invention may be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc. would also be acceptable. Further, other types of interfaces and media could also be used with the router.

Regardless of network device's configuration, it may employ one or more memories or memory modules (including memory **360**) configured to store program instructions for the network operations and network access and control functions described herein. The program instructions may specify an operating system and one or more applications, for example. Such memory or memories may also be configured to store, for example, control information for controlling in-room control systems, etc.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). The invention may also be embodied in a carrier wave travelling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Referring back to FIG. **3b**, HEM **124** has a plurality of ports **126** each of which communicates with a corresponding IRM **104**. HEM **124** has the ability to sense when any of ports **126** are being used so that the hotel may bill the user accordingly. This monitoring feature is also useful for technical support, network bandwidth requirement estimates, billing estimates, and buying pattern data. HEM **124** also has the capability of enabling and disabling individual ports **126**. Where network **100** is part of a wide area network (as discussed below), the monitoring, enabling, and disabling of ports **126** may be done from a remote server at the center of the WAN.

As described above, each HEM port **126** (and thus the corresponding IRM **104**) has a fixed IP address which may be configured using SNMP. The fixed IP address of the HEM port **126** and the IRM **104** is assigned to the guest's computer using DHCP. Alternatively, an address translation is performed between the computer's internal IP address and the fixed IP address of IRM **104**/HEM port **126**. HEM **124** has a small boot ROM **378** for basic IP communications and a large flash ROM **380** for fully functional software and configuration data. This allows for remote software upgrades using, for example, an encrypted protocol riding on top of IP.

According to various embodiments, HEM **124** also comprises transmission circuitry **316** for transmitting and receiving data on a single twisted pair of conductors. Thus, the Ethernet data which has been combined with the standard telephone signals at IRM **104** may be picked off and reconfigured for transmission according to standard Ethernet techniques. Also, data headed to IRM **104** may be combined for transmission over the single twisted pair. As with trans-

US 6,996,073 B2

11

mission circuitry **308**, transmission circuitry **316** may be implemented according to the home PNA standard.

FIG. **5** is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a chain of hotels **502** according to one embodiment of the invention. Using the internal infrastructure described above with reference to FIG. **1**, each hotel **502** has a local area network (LAN) (not shown) which provides direct access to the Internet **504** for each of its guest rooms. According to this embodiment, each hotel **502** must provide its own security in the form of a firewall **506** for the protection of its LAN.

FIG. **6** is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a chain of hotels **602** according to another embodiment of the invention. Using the internal infrastructure described above with reference to FIG. **1**, each hotel **602** has a LAN (not shown) which is then connected with other LANs in the other hotels **602** to form a wide area network (WAN) referred to herein as a virtual private network (VPN) **604**. According to a specific embodiment, VPN **604** is built on an optical fiber backbone employing asynchronous transfer mode (ATM) technology to transmit data packets. It will be understood however that any of a variety of transmission protocols and infrastructures may be employed to transmit data in such a network without departing from the scope of the present invention. Such protocols may include but are not limited to frame relay, Ethernet, and FDDI. Data are configured in the appropriate format as they leave each hotel **602** by a framer (not shown) which may be part of or associated with each hotel's router or file server.

The embodiment of FIG. **6** provides several advantages over the embodiment described above with reference to FIG. **5**. High speed access to the Internet requires some form of connection to the Internet such as, for example, a T1 or T3 line. Not only does such a connection require a hardware infrastructure to support it, it also necessitates some form of protection for the network in the form of, for example, a firewall. Thus, if each hotel property in a hotel chain were to be directly connected to the Internet (as shown in FIG. **5**), each property would need to have its own network hardware infrastructure, firewall, and the technical and administrative staff and functions to support the same. By contrast, with VPN **604**, access to the Internet **606** is provided via a single network center (represented by remote network operation center (NOC) server **608**) at which one or more firewalls **610** and any other necessary networking hardware and equipment may be located and managed. According to a specific embodiment, a redundant network center is provided in a different city than the first against the event that one or the other goes down.

Having each hotel property directly connected to the Internet is problematic for effecting control of the hotels from a central location. That is, the more each hotel LAN is amenable to control from a central location, the more vulnerable it is to hacking. With VPN **604**, security is complete and centralized control is virtually unlimited. This makes things like remote software upgrades convenient thus eliminating what might otherwise be significant field service costs. In addition, because much of the equipment is centrally located, the costly redundancy of equipment and support functions at each hotel property made necessary by the embodiment of FIG. **5** is avoided.

Another important benefit of VPN **604** relates to the management of globally unique IP addresses. As mentioned above, there is a paucity of pools of globally unique IP addresses which are sufficiently large to accommodate each host on the networks of most medium to large size organi-

12

zations. For example, one pool of class C addresses accommodates less than 256 simultaneous users on a network. This might be sufficient at most hotels much of the time, but it is clear that there are foreseeable circumstances where it would not be. For example, as mentioned above, if a 1200 room hotel hosted an Internet technologies seminar it is highly likely that such a pool of addresses would not be sufficient. In addition, this scenario makes the assumption that each property in a hotel chain (some comprising over 1000 properties) could procure a pool of class C addresses.

VPN **604** addresses this problem in that it spreads the IP address needs of each of the hotel properties over the resources of the entire wide area network. Thus, for example, a single class B pool of addresses might be used to accommodate all of the Internet access needs of an entire hotel chain even where the total number of rooms in the chain far exceeds the number of available globally unique IP addresses. That is, large bursts of IP address needs may occur simultaneously at dozens of the hotel properties without exhausting the nearly 64,000 globally unique addresses available in the class B pool.

Other secure services may also be provided via VPN **604**. For example, video teleconferencing-over-IP **612** and voice-over-IP communications **614** may be provided to hotel guests. Moreover, by arranging access to VPN **604** by corporate hosts **616**, individual employees of those corporations can have secure access to their employer's network from remote locations. Other services such as, for example, property management services **618** may be provided to the management of hotels **602**.

FIG. **7** is a block diagram illustrating an auto-bauding technique which may be employed with certain alternative embodiments of the present invention. FIG. **8** is a flowchart **800** illustrating the same. Every transmission line in a hotel's wiring infrastructure has different transmission characteristics due to its length and proximity to sources of distortion. Therefore, according to a specific embodiment of the invention in which an alternative to the home PNA standard is employed, IRM **702** and HEM **704** are operable to determine the maximum data rate for each guest room individually. That is, instead of using a single rate to accommodate the slowest transmission line in the network, each room is allowed a data rate which is the maximum allowed by its transmission line. On power, IRM **702** goes to its lowest baud rate, i.e., 128 kHz (**802**). HEM **704** transmits empty packets at 400 microsecond intervals while IRM listens at its current baud rate (**804**). If communication is not established (**806**), an error message is generated notifying the network administrator that IRM **702** is not operational (**808**). If, however, communication is established (**806**), HEM **704** instructs IRM **702** to baud up to the next higher rate (**810**). If communication is established at the next higher rate (**812**), HEM **704** again instructs IRM **702** to baud up to the next higher rate (**810**). This occurs iteratively until a baud rate is reached at which communication cannot be established. At that point, IRM **702** returns to the lowest baud rate (**814**) and HEM **704** instructs IRM **702** to baud up to the highest baud rate at which communication was established (**816**). In this way, data to and from IRM **702** will always be transmitted at the maximum allowable rate.

FIG. **9** is a flowchart **900** illustrating the customization of a guest room and the transmission of control information to in-room systems via a hotel network. The ability of the present invention to provide half duplex data to each guest room over a single twisted pair connection provides additional advantages which are likely to engender further hotel customer loyalty. In recent years, the hospitality industry has

US 6,996,073 B2

13

been looking for customization solutions to tailor guest rooms to the needs and preferences of the individual guest. The belief is that this would go a long way toward creating the type of customer loyalty with the business traveler that airlines have created with frequent flyer programs. The basic idea is that a hotel or hotel chain keeps a database record for frequent guests in which a variety of parameters may be specified such as, for example, room temperature, lighting, background music, etc. Other customization options include various information services preferred by the guest such as, for example, stock quotes, weather reports, entertainment calendars, etc. When the guest checks in, the assigned room is then automatically configured to suit that guest's preferences.

One method of configuring the room automatically involves adjusting various controls in the room via remote control signals such as, for example, radio frequency (RF) or infrared signals. According to a specific embodiment of the invention, control signals are sent to the IRM (e.g., IRM 104 of FIGS. 1 and 3a) in the guest room via the hotel network where they are converted to the appropriate form, e.g., RF, and used to set the room controls appropriately. In this way, the room's thermostat, light controls, and stereo controls may be set to provide a comfortable and familiar environment for the newly arrived guest. And, because the present invention allows half duplex data to be combined with standard telephone signals, the transmission of room control signals may be done in this manner even where the hotel wiring consists of only single twisted pair technology. In addition and as described above, digital audio and video signals as well as digital information services may be sent to the room in the same manner providing further customization capabilities. Thus, the guest room customization solution of the present invention provides a powerful tool by which individual hotels and hotel chains may engender greater customer loyalty and thereby realize increased revenues.

Referring now to FIG. 9, a specific embodiment of the invention will now be described. As described above, specific information for an individual guest is maintained in a database record 901 either on the server of a specific hotel or on a central remote server from which it may be downloaded to the specific hotel at which the corresponding guest is scheduled to arrive or is actually checking in (902). As the guest is checking in or in response to some other appropriate event, information regarding the guest's room environment and other preferences in database record 901 is transmitted from the HEM to the IRM in the guest's assigned room (904). The information is transmitted via the hotel network which may comprise the hotel's single twisted pair telephone wiring infrastructure. The in-room module then displays some of the received information, e.g., stock quotes, and converts some of the received information into an appropriate set of control signals, e.g., RF signals, for communicating with the room's various environmental controls (906). These environmental controls may include, for example, the thermostat, lighting controls, stereo controls, television controls, etc. The appropriate adjustments are then made to the various systems in the guest room to provide the optimal environment specifically suited to the stated preferences of the arriving guest (908).

FIG. 10 is a block diagram of a file server 1000 for use with various embodiments of the present invention. File server 1000 may be used, for example, to implement any of HEM 124 of FIGS. 1 and 3a, firewall 506 of FIG. 5, and firewalls 610 and remote server 608 of FIG. 6. File server 1000 includes display 1002 and keyboard 1004, and mouse

14

1006. Computer system 801 further includes subsystems such as a central processor 1008, system memory 1010, fixed disk storage 1012 (e.g., hard drive), removable disk 1014 (e.g., CD-ROM drive), display adapter 1016, and network interface 1018 over which LAN, WAN, and Internet communications may be transmitted. File server 1000 operates according to network operating system software and may perform other functions such as, for example, file and database management. Other systems suitable for use with the invention may include additional or fewer subsystems. For example, another system could include more than one processor 1008 (i.e., a multi-processor system), or a cache memory (not shown).

The system bus architecture of file server 1000 is represented by arrows 1020. However, these arrows are illustrative of any interconnection scheme serving to link the subsystems. For example, a local bus could be utilized to connect the central processor to the system memory. File server 1000 is but an example of a system suitable for use with the invention. Other architectures having different configurations of subsystems may also be utilized.

Various embodiments of the present invention may be used to provide special levels of service to specific groups such as, for example, the attendees of a conference at a hotel property. That is, conference attendees are identified when they connect to the hotel network and are provided access to specific content and online services which are related to the conference. FIG. 11 is a flowchart 1100 illustrating the providing of such online conference services using various ones of the network infrastructures described above such as, for example, the network environments of FIGS. 1, 3a, 3b, 5 and 6. A group identification number or tag is associated with each of the attendees of a specific conference (1102). According to a specific embodiment, this is accomplished by associating the network addresses of the IRMs in each of the guest rooms occupied by one of the attendees with the group ID tag. Conference specific services and content are then provided on the network (1104).

Conference services might include, for example, substantially real time voice communication and/or video teleconferencing with other attendees of the conference. Speakers or conference organizers may have software they want to distribute to attendees electronically. Only conference attendees have access to such electronic information. Conference specific content such as, for example, electronic copies of papers presented at the conference as well as PowerPoint® presentations are provided. Individual presenters at the conference can post follow up notes and answers to questions they were not able to get to during their presentation. Chat Rooms could be provided in which, at the end of the day, conference members can get online from their room to interact with other members. Only conference members would have access to the chat room. This service allows conference attendees to discuss questions and comments about the conference, talk about the sessions that were good and bad, critique speakers, and in general exchange information with other attendees. According to various embodiments, the chat rooms could be recorded and the information provided to conference organizers to allow them to better serve their members at future conferences. The real names of chat room participants may be excluded from this information. Bulletin boards for the posting of information by any conference attendee may also be provided. Discounted access to other services such as, for example, entertainment and information services, may also be provided.

US 6,996,073 B2

15

As described above with reference to FIG. 2, when a guest's computer connects to an IRM in any one of the guest rooms, the network IP address associated with that IRM is associated with the computer (1106). As discussed above, this association could mean a DHCP assignment of the network IP address to the guest's computer where the computer did not already have an internal IP address. It could also mean that the internal IP address of the computer is translated into the network IP address. This address assignment/translation may be effected by the IRM, the HEM, or a remote server where the hotel is part of a virtual private network as described above with reference to FIG. 6.

If the network IP address associated with a particular guest's computer is associated with the group ID tag (1108), access to the conference specific services and content are provided to the user of that computer (1110). If, on the other hand, the network IP address is not associated with the group ID (1108), access to the conference specific services and content is blocked. The network IP address remains associated with the guest's computer until the session ends, e.g., the computer is disconnected from the IRM or powered down (1114).

The technique described above with reference to FIG. 11 could be used more generally to restrict access to particular services, content, web sites, other networks, etc. to specific identifiable groups. For example, when an employee of a particular corporation checks into the hotel, the network IP address of the IRM in that employee's room may be associated with a group ID tag which will enable access to the corporation's computer (e.g., see computer host 616 of FIG. 6). As will be understood, restriction of access to a variety of content and services in this manner may be effected according to a variety of group identifications without departing from the scope of the present invention.

While the invention has been particularly shown and described with reference to specific embodiments thereof, it will be understood by those skilled in the art that changes in the form and details of the disclosed embodiments may be made without departing from the spirit or scope of the invention. For example, many of the embodiments described herein have been described with reference to hotels. It will be understood, however, that the techniques employed by the present invention may be applied to a variety of structures and institutions such as, for example, schools, office buildings, and the like. In addition, several embodiment described herein employ single twisted pair wiring which is the standard telephone wiring found in most buildings. However, it will be understood that the techniques described herein may be implemented on any of a wide variety of wiring infrastructures including, for example, Ethernet and ATM systems. Therefore, the scope of the invention should be determined with reference to the appended claims.

What is claimed is:

1. A method for providing conference services over a network having a plurality of users associated therewith, selected ones of the plurality of users being associated with network access nodes on the network, each network access node having a network address associated therewith which is unique on the network, the method comprising:

associating a group identification tag with the network addresses thereby identifying the selected users as attendees of the conference;
providing the conference services on the network; and
restricting access to the conference services to the selected users using the group identification tag.

16

2. The method of claim 1 wherein restricting access to the conference services comprises verifying that a particular network address from which a request has been received has the group identification tag associated therewith before providing access to the conference services.

3. The method of claim 1 wherein providing the conference services on the network comprises providing access to conference data content to the selected users via the network.

4. The method of claim 3 wherein the conference data content comprises PowerPoint® presentation data.

5. The method of claim 3 wherein the conference data content comprises electronic copies of written materials.

6. The method of claim 1 wherein providing the conference services on the network comprises providing discounted access to entertainment content.

7. The method of claim 1 wherein providing the conference services on the network comprises providing discounted access to information services.

8. The method of claim 1 wherein providing the conference services on the network comprises providing substantially real time voice communication.

9. The method of claim 1 wherein providing the conference services on the network comprises providing video teleconferencing services.

10. A method for providing conference services over a network having a plurality of network access nodes each having a network address associated therewith which is unique on the network, comprising:

associating the network addresses with computers associated with a plurality of users while the computers are connected to the network access nodes thereby providing access to the network for each of the plurality of users;

associating a group identification tag with the network address associated with selected ones of the plurality of users thereby identifying the selected users as attendees of a conference;

providing the conference services on the network; and
restricting access to the conference services to the selected users using the group identification tag.

11. The method of claim 10 wherein selected ones of the computers have internal IP addresses and associating the network addresses with the selected computers comprises translating the internal IP addresses to the network addresses.

12. The method of claim 10 wherein selected ones of the computers do not have internal IP addresses and associating the network addresses with the selected computers comprises assigning the network addresses to the computers.

13. The method of claim 10 wherein the network comprises a local area network and associating the network addresses is done by a headend associated with the local area network.

14. The method of claim 10 wherein the network comprises a wide area network and associating the network addresses is done by a remote server which controls the wide area network.

15. The method of claim 10 wherein associating the network addresses is done by the network access nodes.

* * * * *

EXHIBIT 3

(12) **United States Patent**
West et al.

(10) **Patent No.:** **US 7,580,376 B2**
(45) **Date of Patent:** ***Aug. 25, 2009**

(54) **METHODS AND APPARATUS FOR
PROVIDING HIGH SPEED CONNECTIVITY
TO A HOTEL ENVIRONMENT**

(75) Inventors: **William B. West**, Salt Lake City, UT
(US); **Wallace Eric Smith**, Lindon, UT
(US); **Steven R. McDaniel**, Salt Lake
City, UT (US)

(73) Assignee: **Ibahn General Holdings Corporation**,
South Jordan, UT (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 525 days.

This patent is subject to a terminal dis-
claimer.

(21) Appl. No.: **11/281,254**

(22) Filed: **Nov. 16, 2005**

(65) **Prior Publication Data**
US 2006/0187861 A1 Aug. 24, 2006

Related U.S. Application Data
(60) Continuation of application No. 10/746,275, filed on
Dec. 23, 2003, now Pat. No. 6,996,073, which is a
division of application No. 09/256,719, filed on Feb.
24, 1999, now Pat. No. 6,738,382.

(51) **Int. Cl.**
H04L 12/16 (2006.01)
H04Q 11/00 (2006.01)
(52) **U.S. Cl.** **370/260; 379/202.01**
(58) **Field of Classification Search** None
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS

5,669,005 A * 9/1997 Curbow et al. 715/234
5,790,548 A 8/1998 Sistanizadeh et al.

5,793,763 A 8/1998 Mayes et al.
5,812,819 A 9/1998 Rodwin et al.
5,835,725 A 11/1998 Chiang et al.
6,011,782 A 1/2000 DeSimone et al.
6,052,725 A 4/2000 McCann et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP 1017208 A2 5/2000

(Continued)

OTHER PUBLICATIONS

European Search Report dated Mar. 23, 2007, from corresponding EP
Application No. EP 00913543.5 (8 pages).

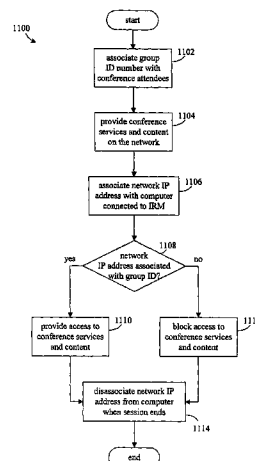
(Continued)

Primary Examiner—Ajit Patel
(74) *Attorney, Agent, or Firm*—Weaver Austin Villeneuve &
Sampson LLP

(57) **ABSTRACT**

Methods and apparatus are described for providing access to
a network via a first one of a plurality of network access nodes
in the network. The network access nodes each have a net-
work address associated therewith which is unique on the
network, the first network access node having a first network
address associated therewith. The first network address is
associated with a first computer while the first computer is
connected to the first network access node thereby providing
access to the network.

15 Claims, 12 Drawing Sheets



US 7,580,376 B2

Page 2

U.S. PATENT DOCUMENTS

6,058,431	A	5/2000	Srisuresh et al.	
6,061,349	A	5/2000	Coile et al.	
6,081,907	A *	6/2000	Witty et al.	714/6
6,118,768	A	9/2000	Bhatia et al.	
6,128,657	A	10/2000	Okanoya et al.	
6,269,081	B1 *	7/2001	Chow et al.	370/241
6,393,017	B1	5/2002	Galvin et al.	
6,614,774	B1	9/2003	Wang	
6,738,382	B1	5/2004	West et al.	
6,850,497	B1	2/2005	Sigler et al.	
6,940,821	B1 *	9/2005	Wei et al.	370/244

FOREIGN PATENT DOCUMENTS

WO WO9840990 9/1998

OTHER PUBLICATIONS

Canadian Office Action dated Jun. 6, 2007, from corresponding CA Application No. 2,363,683 (3 pages).
Borella et al., Internet Draft, Entitled, "Realm Specific IP: Protocol Specification", IETF, Feb. 1999.
K. Egevang et al., "The IP Network Address Translator (NAT)", May 1994, RFC 1631.

International Search Report dated Jun. 13, 2000 from PCT International Application No. PCT/US00/04293.

International Preliminary Examination Report dated Apr. 18, 2001 from PCT International Application No. PCT/US00/04293.

PCT Written Opinion dated Jan. 10, 2001 from PCT International Application No. PCT/US00/04293.

Office Action dated Mar. 8, 2002 from U.S. Appl. No. 09/256,719.

Office Action dated Sep. 11, 2002 from U.S. Appl. No. 09/256,719.

Final Office Action dated Dec. 16, 2002 from U.S. Appl. No. 09/256,719.

Office Action dated Apr. 24, 2003 from U.S. Appl. No. 09/256,719.

Final Office Action dated Jul. 18, 2003 from U.S. Appl. No. 09/256,719.

Notice of Allowance dated Oct. 3, 2003 from U.S. Appl. No. 09/256,719.

Office Action dated May 3, 2005 from U.S. Appl. No. 10/746,275.

Notice of Allowance dated Sep. 7, 2005 from U.S. Appl. No. 10/746,275.

Partial European Search Report from corresponding EP Application No. EP 00913543.5 (4 pages). Jun. 16, 2006.

Supplemental European Search Report from corresponding EP Application No. EP 00913543.5 (5 pages). Aug. 31, 2006.

* cited by examiner

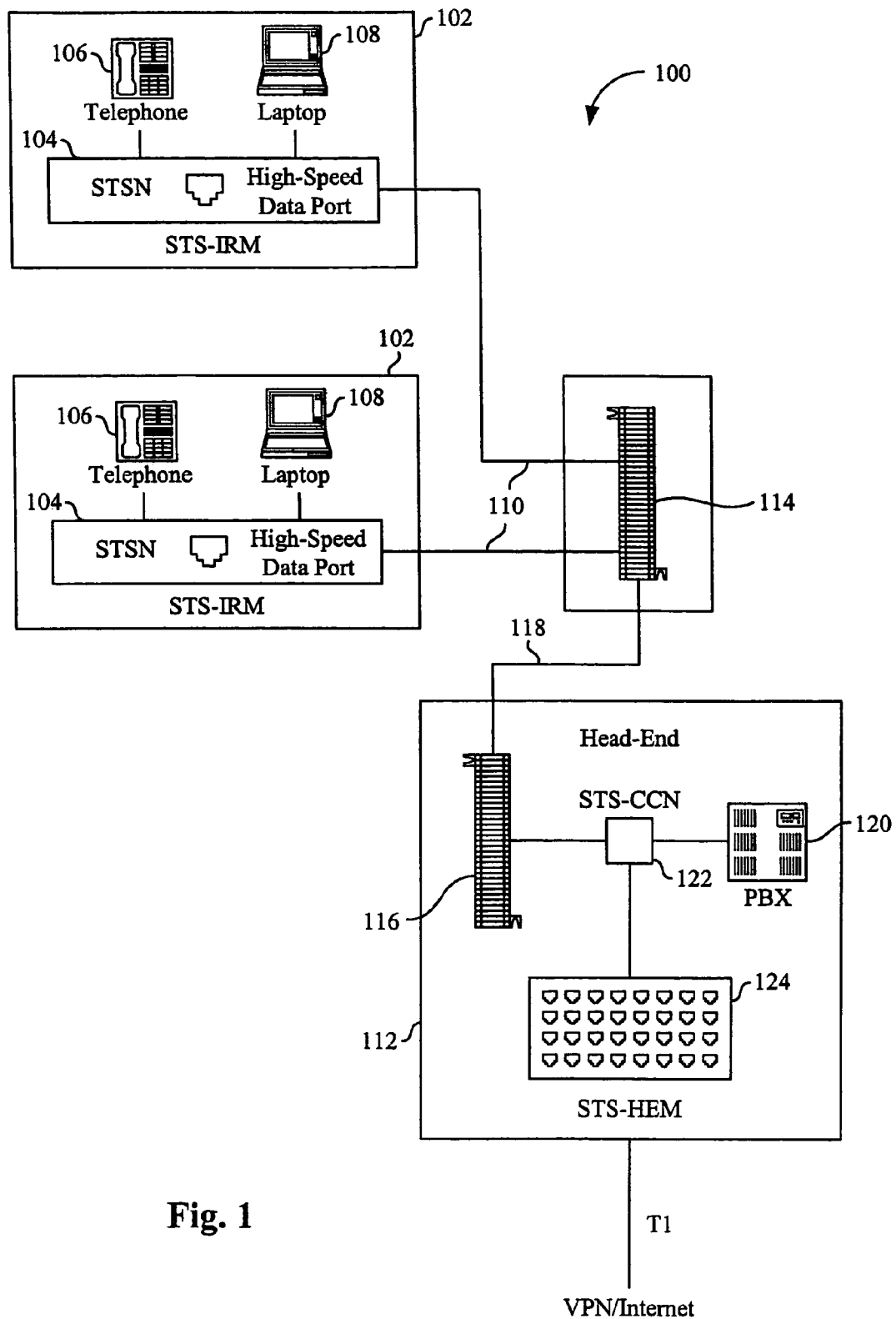
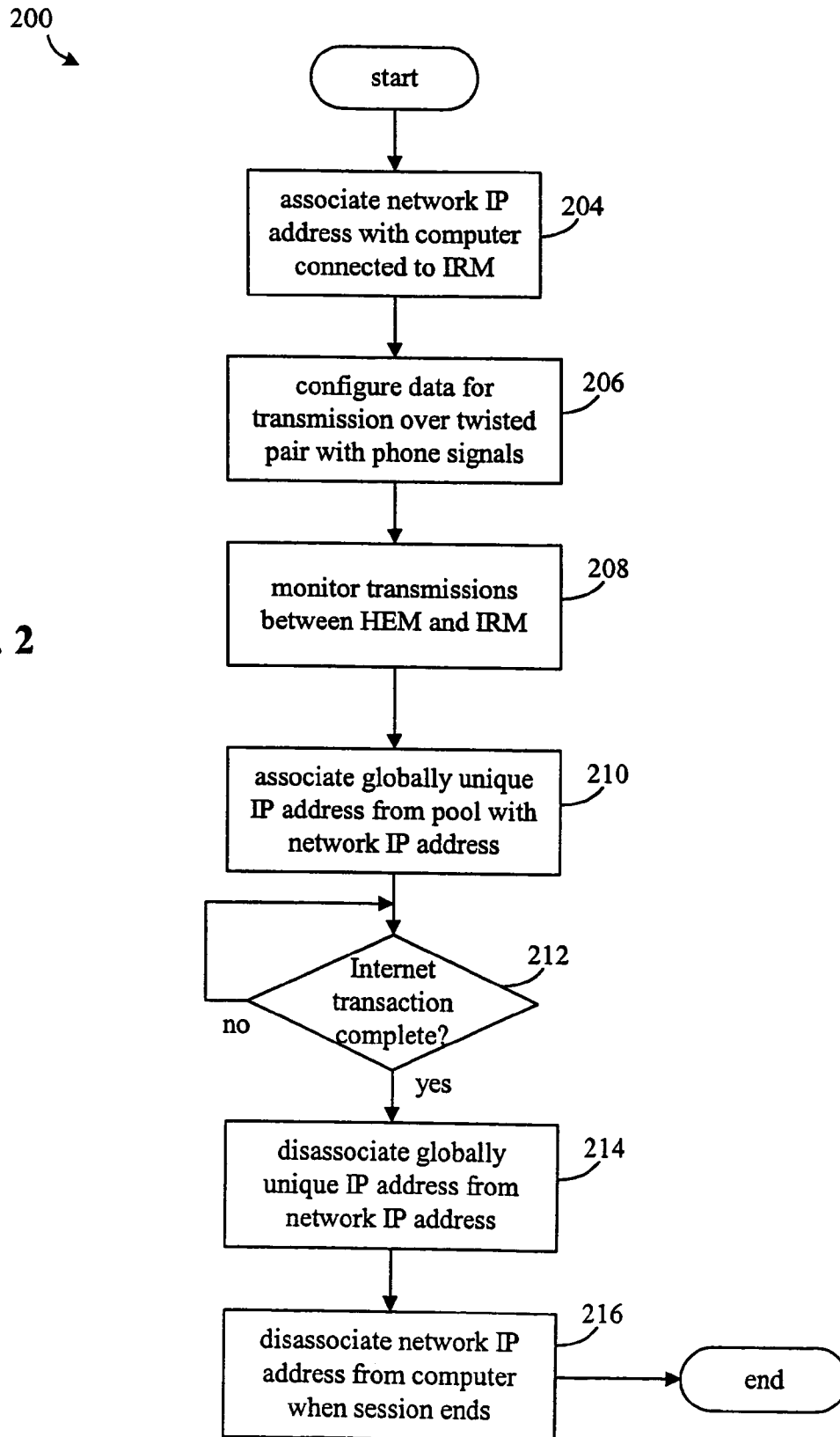


Fig. 1

Fig. 2



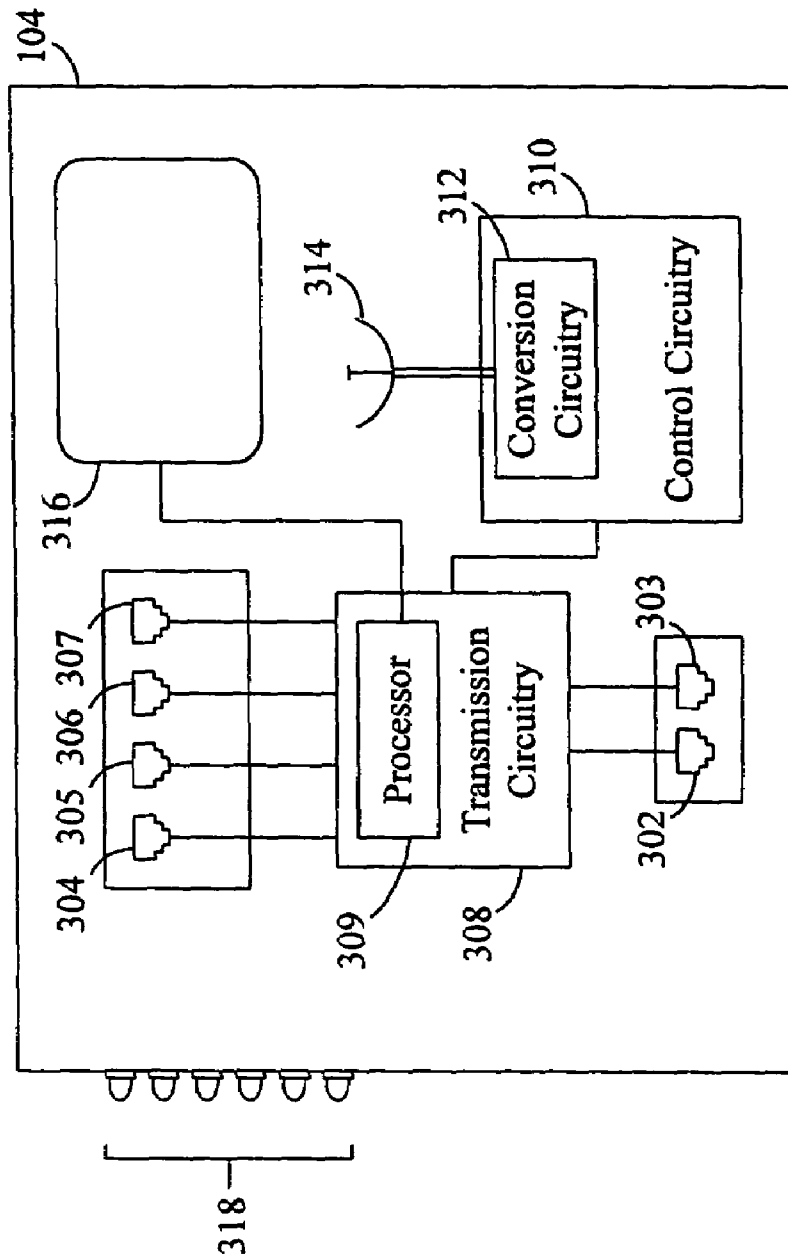


Fig. 3a

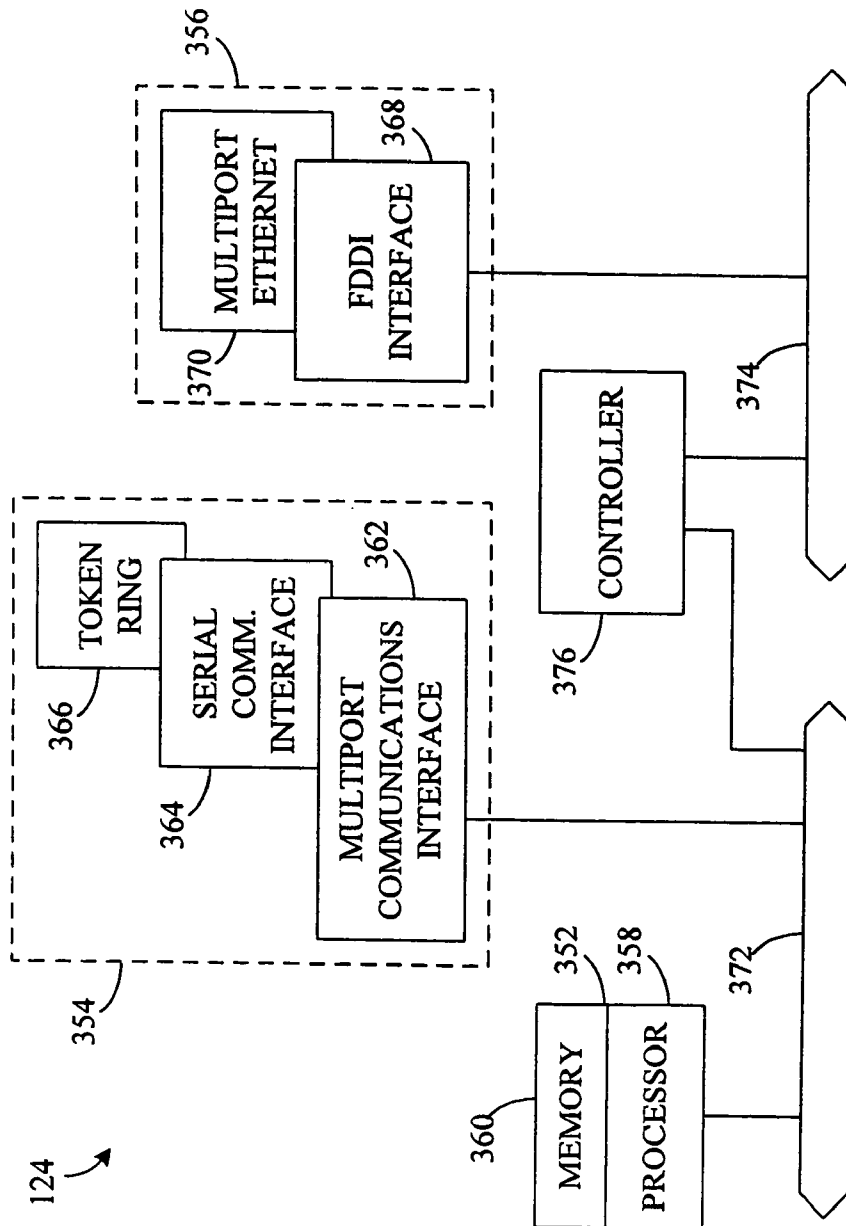


Fig. 3b

U.S. Patent

Aug. 25, 2009

Sheet 5 of 12

US 7,580,376 B2

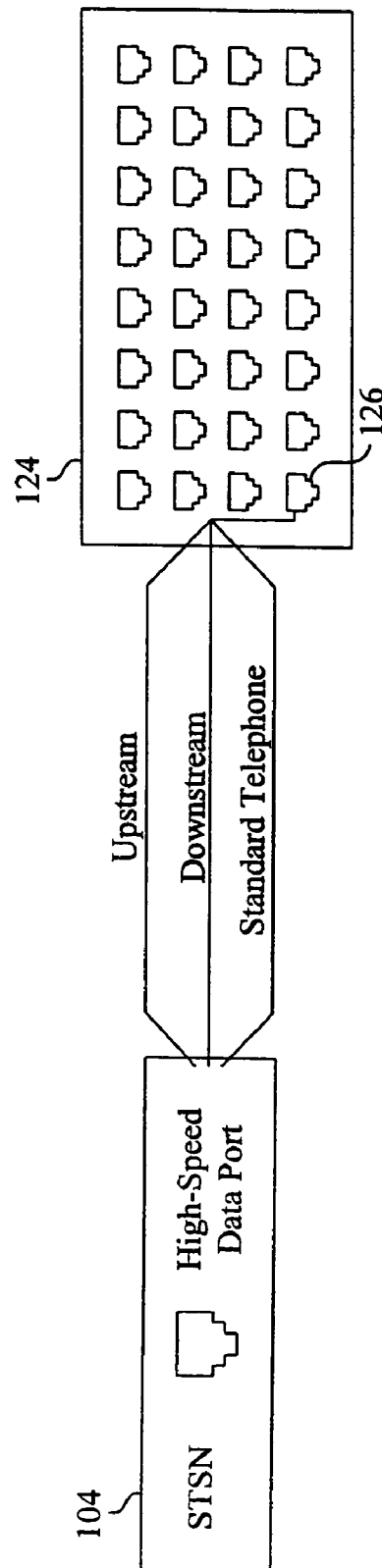


Fig. 4

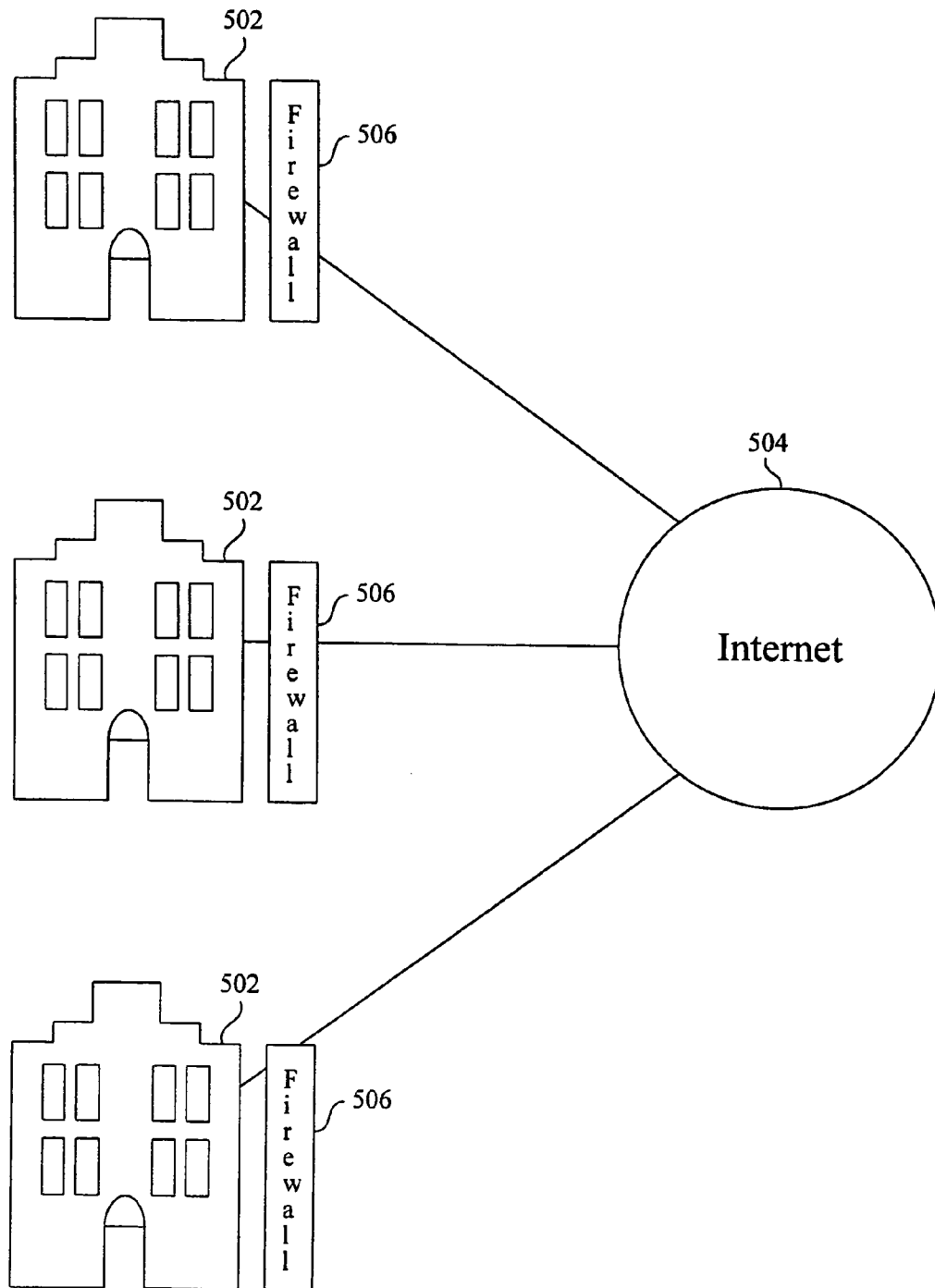


Fig. 5

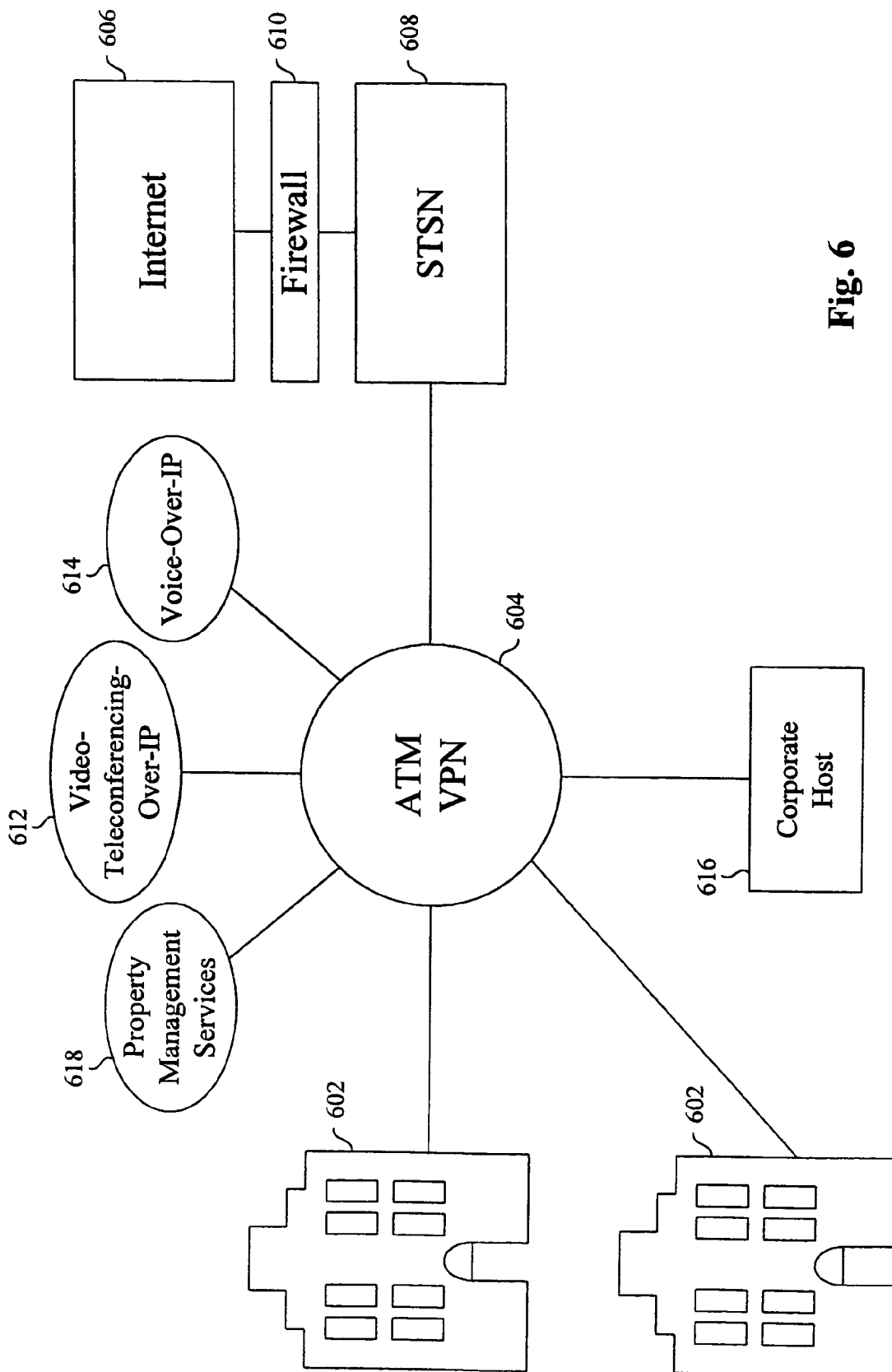


Fig. 6

U.S. Patent

Aug. 25, 2009

Sheet 8 of 12

US 7,580,376 B2

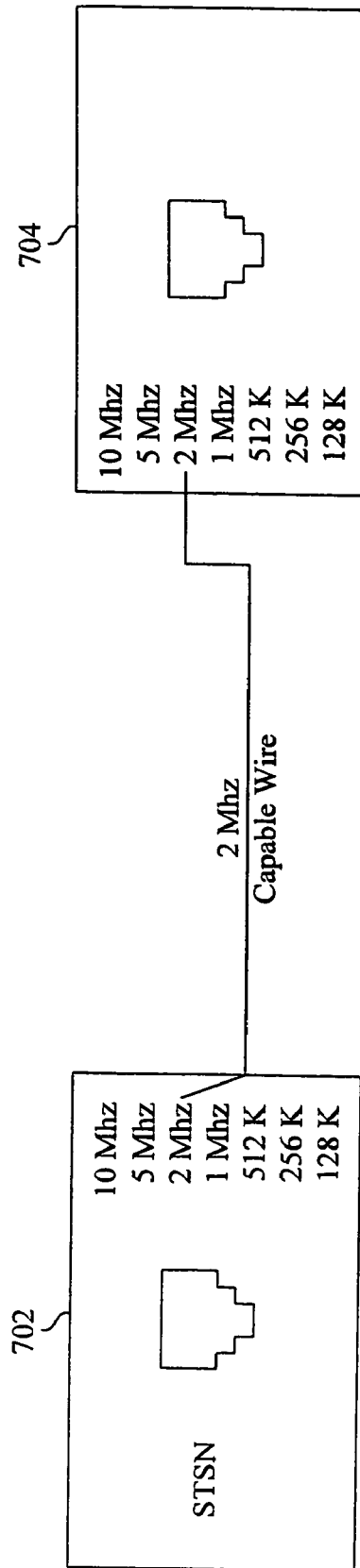
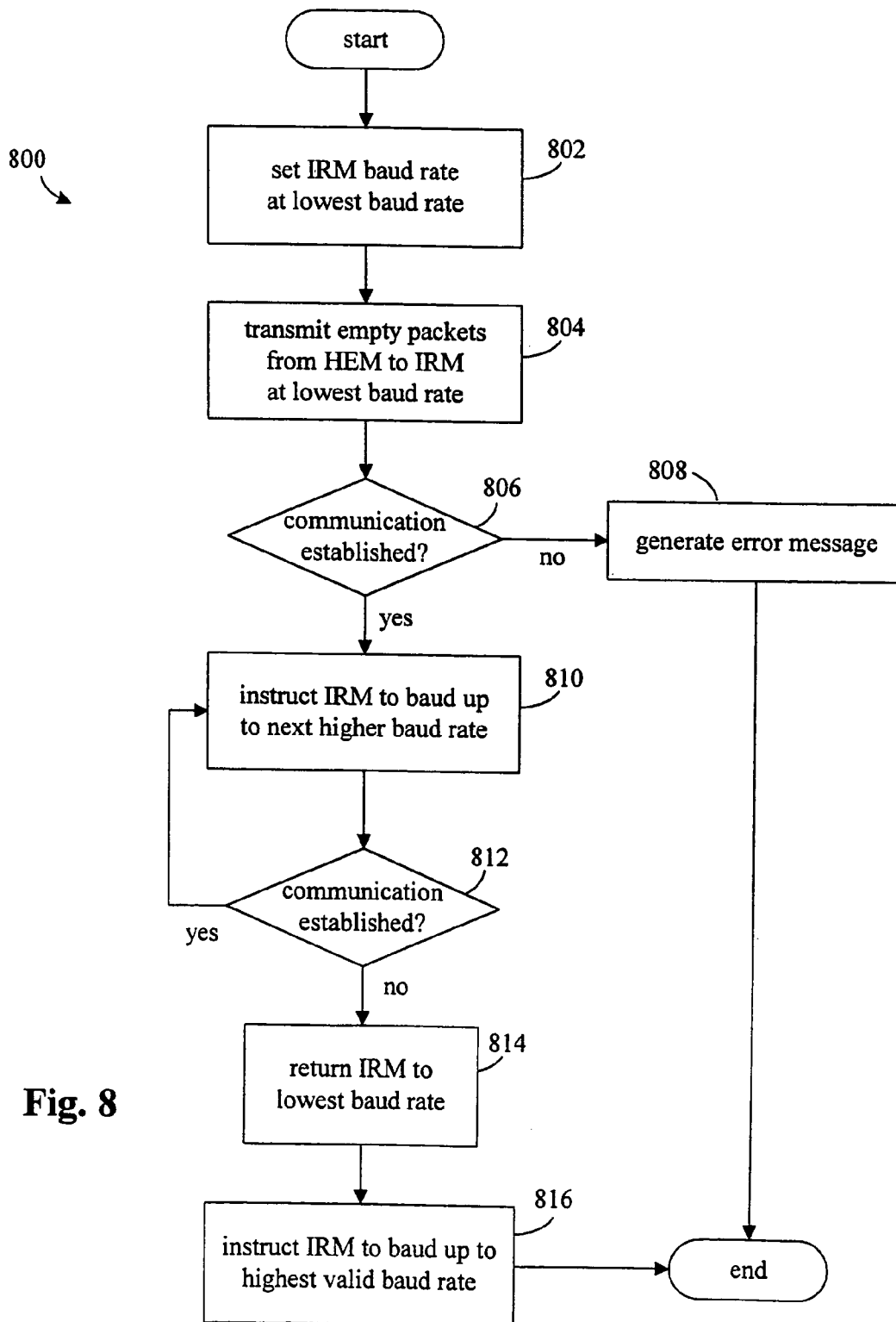


Fig. 7



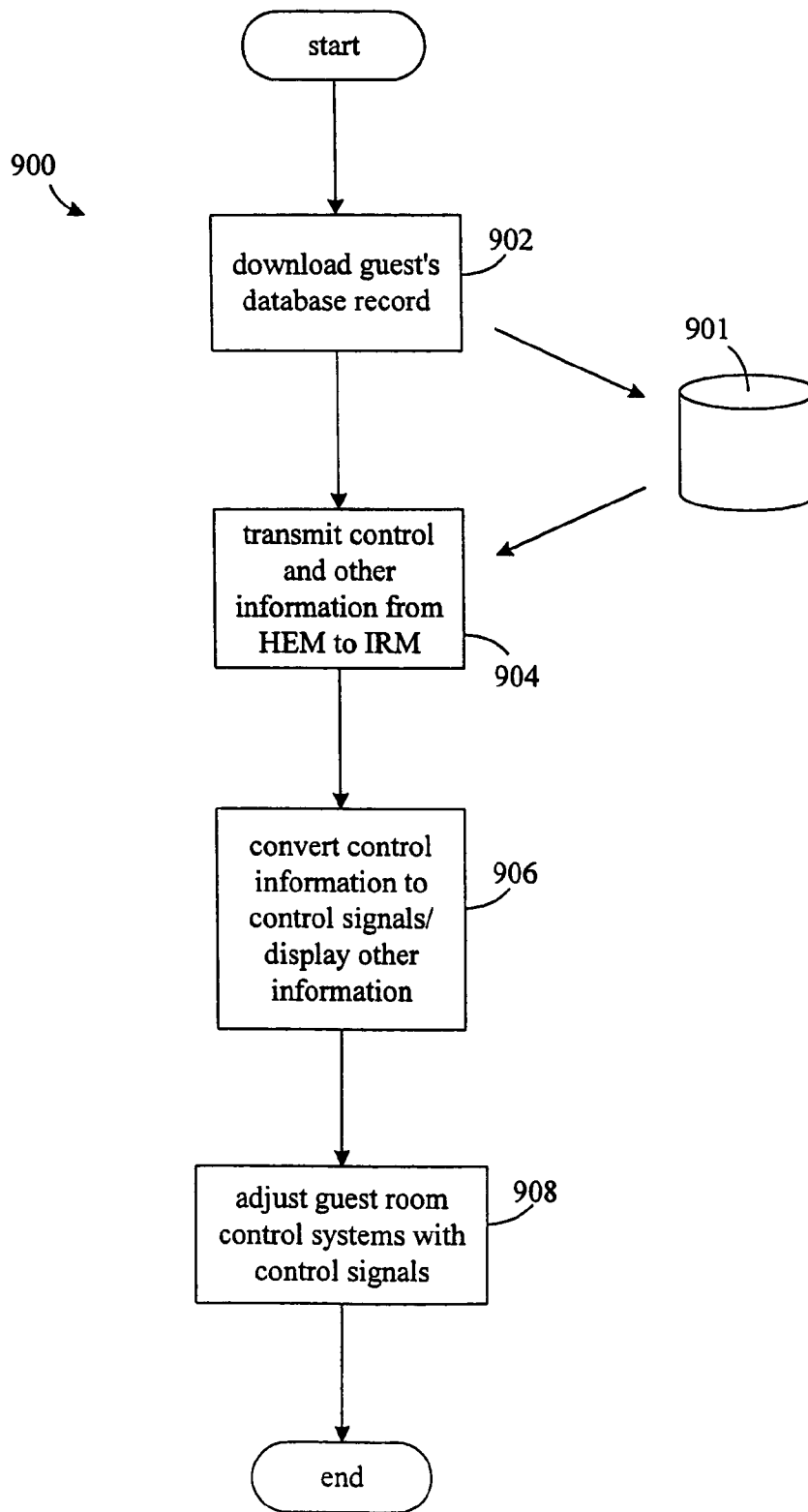


Fig. 9

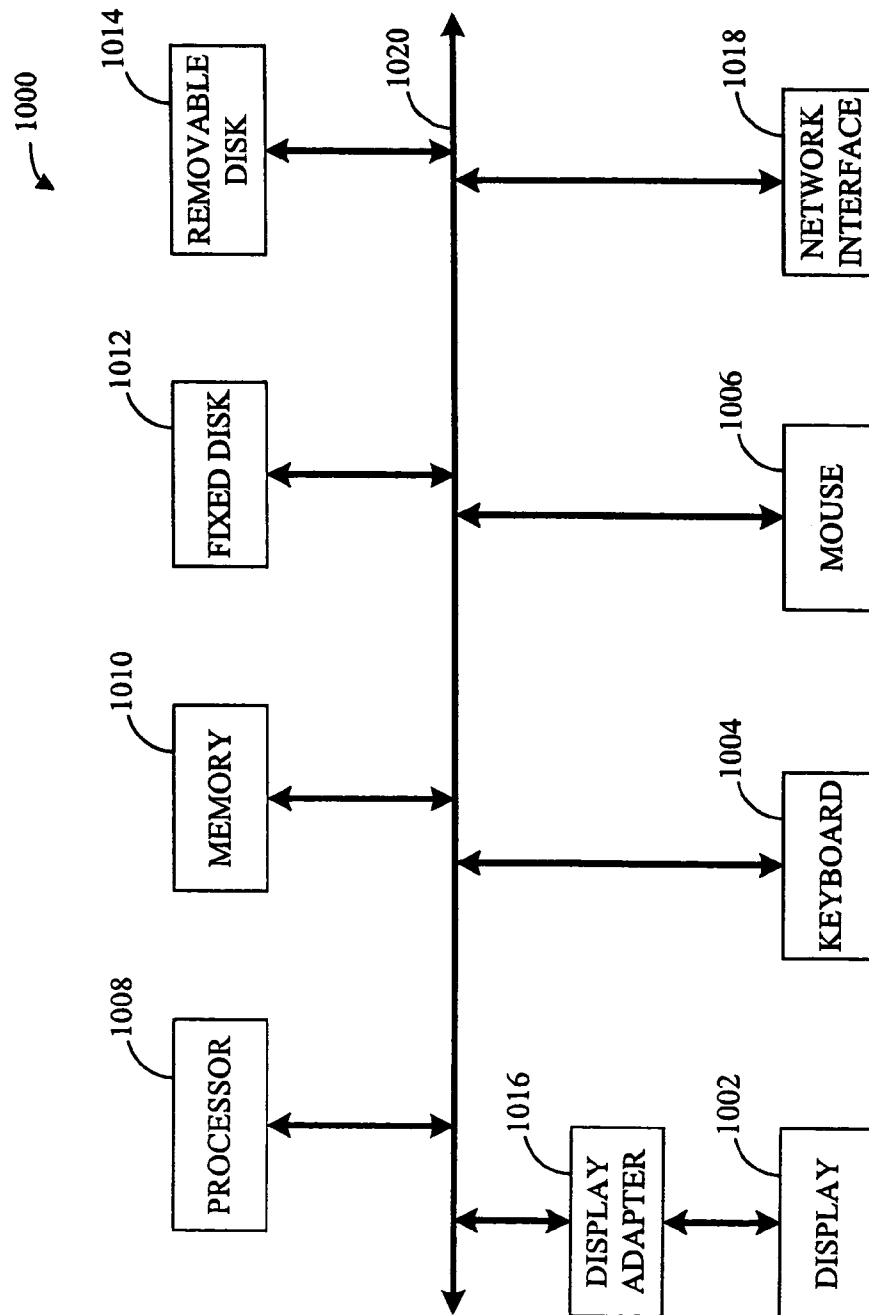


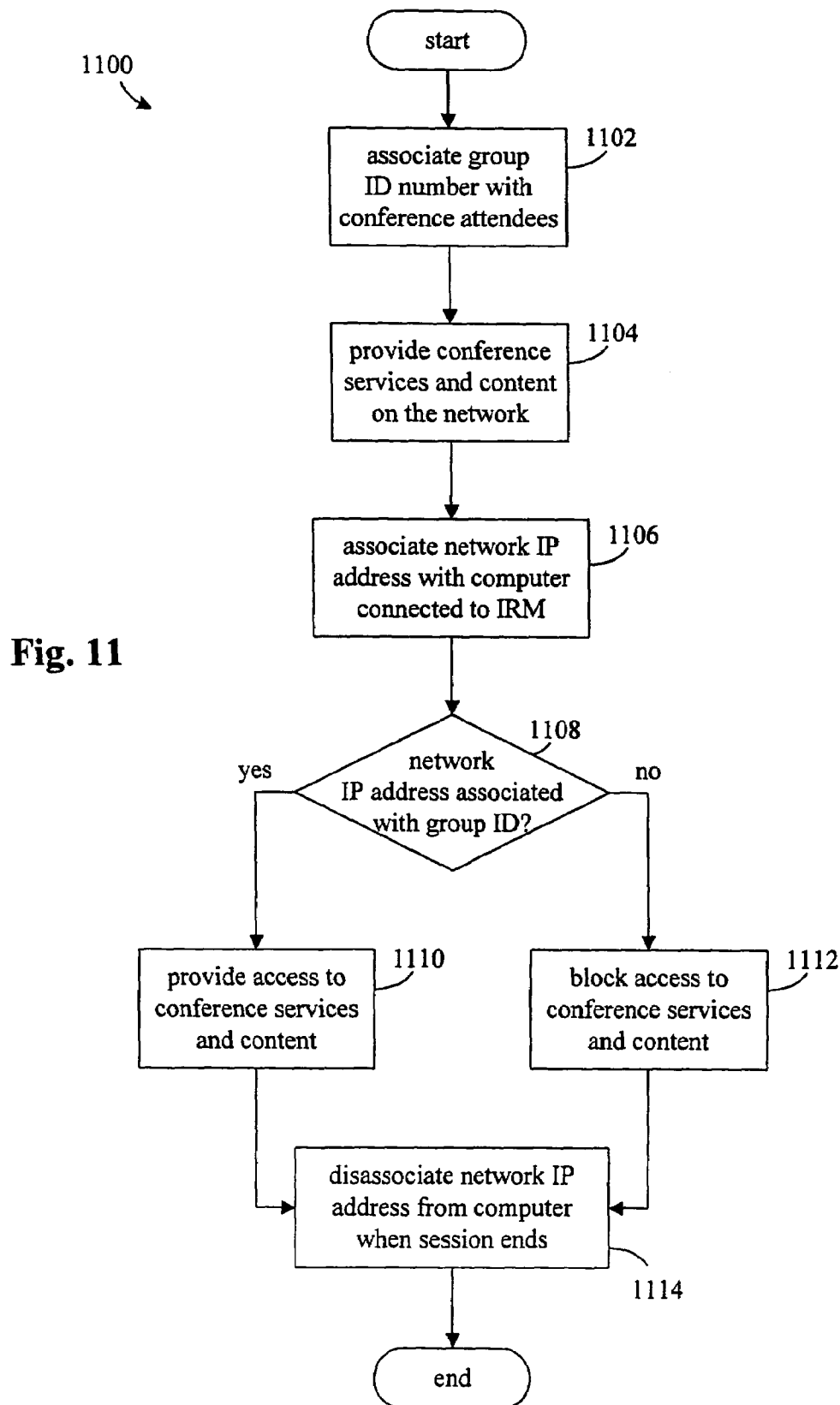
Fig. 10

U.S. Patent

Aug. 25, 2009

Sheet 12 of 12

US 7,580,376 B2



US 7,580,376 B2

1

METHODS AND APPARATUS FOR PROVIDING HIGH SPEED CONNECTIVITY TO A HOTEL ENVIRONMENT

RELATED APPLICATION DATA

The present application claims priority under 35 U.S.C. 120 and is a continuation of U.S. patent application Ser. No. 10/746,275 filed Dec. 23, 2003 now U.S. Pat. No. 6,996,073 which is a divisional of U.S. patent application Ser. No. 09/256,719 filed Feb. 24, 1999 now U.S. Pat. No. 6,738,382, the entire disclosures of both of which are incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

The present invention relates to network communications and, more specifically, to providing high speed Internet access to users in hotel environments.

Any business traveler who relies on network communications to maintain contact with clients and the home office appreciates the availability of fast and reliable data ports at remote locations such as airport lounges and hotel rooms. The hospitality industry has only recently begun to understand the necessity of providing such high speed data connections to business travelers. In fact, given the explosive growth of network technologies and the corresponding dependence of the business professional on such technologies, hotels which do not move to provide high speed connectivity in guest rooms comparable to the typical office environment will likely lose a substantial portion of their business to hotels which do.

Unfortunately, many hotel rooms are not currently wired to accommodate high speed data traffic. That is, prior to 1990, virtually all hotel rooms were wired to provide only basic telephone service. As late as 1995, less than 10% of hotel rooms were wired to handle standard Ethernet data speeds. Even today, while the major players in the hospitality industry are searching for high speed connectivity solutions, the vast majority of hotel guest and conference rooms are still wired with low quality, single pair connections. One obvious solution would be to completely rewire all of the guest and conference rooms in each hotel facility to provide the desired data transmission capabilities. However, given the prohibitive cost of such an undertaking, a less costly solution would be desirable.

Even if such a costly rewiring were undertaken, there are other problems which are not addressed by an infrastructure upgrade. For example, even if a high speed connection to the hotel's host is provided, it will often be the case that a guest's laptop computer would be incompatible with the hotel network in some way. Thus, each guest's laptop must be configured appropriately in order to communicate with the network and with the Internet beyond. This would likely involve loading special software onto a guest's laptop each time the guest wants to go online. Not only would such a process be cumbersome and annoying to the hotel guest, it may also be unacceptable from the guest's point of view in that reconfiguring the laptop may interfere with the current configuration in undesirable ways.

Neither does a costly wiring upgrade address the administrative and security issues related to providing Internet access via a hotel host. That is, high speed Internet access for hotel guests requires a network at the hotel property and some sort of connection between the hotel network and the Internet, e.g., a T1 or T3 line. A firewall at each hotel property would also be required to protect the internal network from unau-

2

thorized access. The existence of the firewall at each property, in turn, requires that most of the control and administration of the local network be performed at the hotel property rather than remotely, thus representing an undesirable redundancy of administrative functions.

Another administrative difficulty related to maintaining each hotel property as a separate Internet host involves the management of IP addresses. Ranges of globally unique 32-bit IP addresses are issued to organizations by a central Internet authority. These addresses are organized in a four octet format. Class A IP addresses are issued to very large organizations and employ the first of the four octets to identify the organization's network and the other three to identify individual hosts on that network. Thus, a class A address pool contains nearly 17 million (2^{24}) globally unique IP addresses. With class B addresses, the first two octets are used to identify the network and the last two to identify the individual hosts resulting in 64,000 (2^{16}) globally unique IP addresses for each organization. Finally, with class C addresses, the first three octets are used to identify the network and the last octet to identify the individual hosts resulting in only 256 (2^8) globally unique IP addresses for each organization.

Unfortunately for many medium to large size organizations (1,000 to 10,000 hosts), it has become very difficult, if not impossible, to obtain anything other than a class C address for their networks due to the fact that the class A and B address spaces have been almost entirely locked up. This problem has been addressed to some extent by the use of a Network Address Translation (NAT) protocol. According to such a protocol, when a local host on an organization's network requests access to the Internet, it is assigned a temporary IP address from the pool of globally unique IP addresses available to the organization. The local host is identified by the globally unique address only when sending or receiving packets on the Internet. As soon as the local host disconnects from the Internet, the address is returned to the pool for use by any of the other hosts on the network. For additional details on the implementation of such a protocol please refer to K. Evegang and P. Francis, *The IP Network Address Translator (NAT), Request for Comments "RFC" 1631*, Cray Communications, NTT, May 1994, the entirety of which is incorporated herein by reference for all purposes.

Such dynamic assignment of IP addresses might be sufficient for certain organizations as long as the number of simultaneous users which require access to the Internet remains below the maximum of 256. However, if, for example, a 1200 room hotel were hosting an Internet technologies seminar it would be extremely likely that the demand for Internet access would exceed the available address pool. All of this also assumes that a major hotel chain would be able to obtain a complete class C pool of addresses for each of its properties; not necessarily a reasonable assumption.

It is therefore desirable to provide methods and apparatus by which each of the properties in a major hotel chain may provide high speed Internet access to each of its guest rooms in a secure, inexpensive, and reliable manner without undue administrative burdens on the individual properties.

SUMMARY OF THE INVENTION

According to the present invention, methods and apparatus are provided which make use of existing hotel wiring infrastructures to provide secure, high speed data and Internet access to each of the guest rooms in a hotel property. Specific implementations of the technology described herein have the ability to auto-baud down to whatever speed the wiring infrastructure will allow thus providing the maximum bandwidth

US 7,580,376 B2

3

allowable by that infrastructure. According to specific embodiments, the present invention is able to select the maximum baud rate appropriate for each individual guest room. According to other specific embodiments, where the wiring to the guest rooms is a single pair phone line, the present invention allows 1 Megabit half duplex data transmissions to coexist on the single pair with standard telephone signals.

According to one embodiment of the invention, each guest room in the hotel is interconnected via the hotel's current wiring infrastructure into a local network. When a guest wishes to access the Internet, he connects his laptop to an in-room module installed in each guest room which temporarily assigns a "fake" local IP address to the guest's laptop. The "fake" local IP address is associated with the in-room module and is unique on the hotel's local network. The address is "fake" in that it is not a valid Internet address and in that it replaces the laptop's own real IP address. The assigned local IP address uniquely identifies the guest's laptop on the hotel network while that laptop remains connected to the in-room module.

A headend module in the hotel handles packet routing and provides access to the Internet. In facilitating access to the Internet, the headend module temporarily assigns globally unique IP addresses from a pool of, for example, class C addresses to in-room modules in individual guest rooms in response to requests for Internet access from those rooms. An assigned IP address remains dedicated to a particular in-room module (and thus the associated guest's computer) for the duration of the Internet transaction. Upon termination of the transaction, the globally unique IP address is disassociated from the in-room module and put back into the pool for use in facilitating a later Internet transaction from any of the hotel's rooms.

According to another embodiment of the invention, the local networks of a number of hotels are interconnected via a remote server thereby forming a private wide area network, or a virtual private network. The operation of the virtual private network to provide high speed data and Internet access to individual guest rooms is similar to the process described above except that the "fake" IP address of the in-room modules are unique over the entire virtual private network, and the temporary assignment of globally unique IP addresses is performed by the remote server rather than the hotel headend. This is advantageous in that it is contemplated that the remote server has a larger pool of such addresses associated therewith than an individual hotel network might be able to procure (e.g., a class B address pool).

Thus, because the IP address needs of all of the hotels in the virtual private network are spread out over the entire installed base of the remote server, bursts of need at any one property which exceed the capacity of a single class C address pool may be accommodated. The virtual private network embodiment of the present invention also has the advantage that firewall security and other network administrative functions may be centralized and performed remotely without compromising the security of any individual hotel network.

Thus, according to the present invention, methods and apparatus are provided for providing access to a network via a first one of a plurality of network access nodes in the network. The network access nodes each have a network address associated therewith which is unique on the network, the first network access node having a first network address associated therewith. The first network address is associated with a first computer while the first computer is connected to the first network access node thereby providing access to the network.

4

According to a more specific embodiment, Internet access is provided to a first computer via a first one of a plurality of network access nodes in a network using a plurality of globally unique IP addresses. The network access nodes each have a network address associated therewith which is unique on the network, the first network access node having a first network address associated therewith. The first network address is associated with the first computer while the first computer is connected to the first network access node thereby providing access to the network. A first one of the globally unique IP addresses is associated with the first network address for conducting an Internet transaction. The first globally unique IP address is disassociated from the first network address upon termination of the Internet transaction. The first globally unique IP address is then available for association with any of the network addresses. According to one embodiment, the network comprises a local area network and the associating and disassociating of the globally unique IP address is done by a headend associated with the local area network. According to another embodiment, the network comprises a wide area network and the associating and disassociating of the globally unique IP address is done by a remote server which controls the wide area network.

According to a specific embodiment, a network is provided having a plurality of network access nodes each having a network address associated therewith which is unique on the network. Each network access node is for providing access to the network for a computer connected to the network access node. A headend module interconnects the network access nodes. The network address associated with each network access node is associated with the computer connected thereto thereby providing access to the network.

According to another specific embodiment, a wide area network is provided having a plurality of networks each comprising a plurality of network access nodes. Each network access node has a network address associated therewith which is unique among the plurality of networks. Each network access node provides access to the wide area network for a computer connected to the network access node. A remote server interconnects the plurality of networks into the wide area network. The network address associated with each network access node is associated with the computer connected thereto thereby providing access to the wide area network.

According to yet another specific embodiment, a network access node is provided for providing access to a network of which the network access node is a part. The network access node has a network address associated therewith which is unique on the network. According to a more specific embodiment, the network address node is operable to associate the network address with a computer while the computer is connected to the network access node thereby providing access to the network.

According to a further specific embodiment, a headend module is provided for interconnecting a plurality of network access nodes in a network. Each network access node has a network address associated therewith which is unique on the network and provides access to the network for a computer connected to the network access node. According to a more specific embodiment, the headend module associates the network address associated with each network access node with the computer connected thereto thereby providing access to the network.

According to another specific embodiment, methods and apparatus are provided for providing conference services over a network having a plurality of users associated is therewith. A group identification tag is associated with selected

EXHIBIT 3

PAGE 62

US 7,580,376 B2

5

ones of the plurality of users thereby identifying the selected users as attendees of the conference. The conference services are provided on the network. Access to the conference services is then restricted to the selected users using the group identification tag.

A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a hotel according to a specific embodiment of the invention;

FIG. 2 is a flowchart illustrating a method for providing high speed data and Internet access to guest rooms in a hotel according to a specific embodiment of the invention;

FIGS. 3a and 3b are more detailed block diagrams of the in-room module and head-end module of FIG. 1;

FIG. 4 is a block diagram illustrating the combination of half duplex data and standard telephone data on a single pair of conductors according to a specific embodiment of the invention;

FIG. 5 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in hotels according to another specific embodiment of the invention;

FIG. 6 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in hotels according to yet another specific embodiment of the invention;

FIG. 7 is a block diagram illustrating the auto-bauding technique of the present invention;

FIG. 8 is a flowchart illustrating the auto-bauding technique of the present invention;

FIG. 9 is a flowchart illustrating the customization of a guest room and the transmission of control information to in-room systems via a hotel network;

FIG. 10 is a block diagram of file server for use with various embodiments of the present invention; and

FIG. 11 is a flowchart illustrating the providing of online conference services.

DESCRIPTION OF SPECIFIC EMBODIMENTS

FIG. 1 is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a hotel network 100 according to a specific embodiment of the invention. In each guest room 102 is an in-room module (IRM) 104 by which a telephone 106 and a guest's laptop computer 108 may be connected to the hotel's wiring infrastructure. According to a specific embodiment, IRM 104 is plugged directly into the room's phone jack and has at least two additional ports, one for the room's telephone, e.g., an RJ-11 jack, and one for the guest's laptop, e.g., an RJ-45 Ethernet port. According to various embodiments, IRM 104 performs a number of functions including, for example, combining and separating Ethernet data and standard telephone signals for transmission over the hotel's wiring infrastructure. According to other embodiments and as discussed below, IRM 104 is configured to receive control information from a central location for automated control of various room environmental parameters, e.g., temperature and lighting. According to still other embodiments, IRM 104 is configured to receive a wide variety of other types of data such as, for example, digital audio and video for presentation in the guest room, or a wide variety of other information services.

6

Transmission line 110 connects IRM 104 to the hotel's head-end 112 via any of a wide variety of infrastructures. In the example shown, transmission line 110 connects IRM 104 to head-end 112 via standard telephone company wiring as represented by punch down blocks 114 and 116 and telephone company transmission line 118. It will be understood, however, that the wiring between IRM 104 and head-end 112 may take other forms such as, for example, a four-conductor Ethernet network. Head-end 112 comprises punch down block 116 and public branch exchange (PBX) 120. Interposed between punch down block 116 and PBX 120 is a connection port 122 which, according to a specific embodiment, may be easily installed simply by unplugging the standard 24-pin connector from PBX 120, plugging connection port 122 into the PBX connector (not shown), and plugging the original connector from punch down block 116 into connection port 122. Standard telephone signals pass through connection port 122 to PBX 120 while half duplex Ethernet data packets are transmitted and received by head-end module (HEM) 124.

Depending on the configuration of the present invention, HEM 124 performs a variety of functions and, according to some embodiments, can be thought of as an enhanced router with additional capabilities programmed into its operating system. That is, according to such embodiments, HEM 124 serves as a switch which routes data packets to and from IRMs 104, and serves as the other end of the communications to and from IRMs 104 in which Ethernet data and phone signals are combined over single twisted pair technology. According to other alternative embodiments, HEM 124 handles address translation and assignment, controls network access, and serves as a bridge for Ethernet data transmitted over the hotel's single twisted pair infrastructure. HEM 124 has a plurality of ports 126 each of which communicates with a corresponding IRM 104. This communication may be individually monitored and controlled (by either the IRM or the HEM) thus allowing central hotel management of billing and access as well as the ability to generate reports for troubleshooting purposes.

Each IRM 104 (and thus the corresponding HEM port 126) has a fixed IP address which may be configured using the Simple Network Management Protocol (SNMP). If the guest's computer connected to a particular IRM 104 does not have its own internal IP address, the fixed IP address of the corresponding IRM 104/HEM port 126 is assigned to the guest's computer using the Dynamic Host Configuration Protocol (DHCP) to facilitate access to network 100. If the guest's computer already has its own internal IP address, address translation is performed between the computer's internal IP address and the fixed IP address of the IRM 104/HEM port 126. According to various embodiment of the invention, this address translation may be performed by either IRM 104 or HEM 124. HEM 124 has a small boot ROM (not shown) for basic IP communications and a large flash ROM (not shown) for fully functional software and configuration data. This allows for remote software upgrades using, for example, an encrypted protocol riding on top of IP.

FIG. 2 is a flowchart 200 illustrating a method for providing high speed data and Internet access to guest rooms in a hotel using the system of FIG. 1. When a guest's computer connects to an IRM in any one of the guest rooms, the network IP address associated with that IRM is associated with the computer (204). As discussed above, this association could mean a DHCP assignment of the network IP address to the guest's computer where the computer did not already have an internal IP address. It could also mean that the internal IP address of the computer is translated into the network IP address. This address assignment/translation may be effected

US 7,580,376 B2

7

by either the IRM and the HEM. In addition, it will be understood that depending on where the assignment/translation occurs it may precede or follow 206 described below. The network IP address is associated with the guest's computer while it remains connected to the IRM.

Where the transmission line connecting the IRM to the hotel network comprises a single twisted pair of conductors, the data communications between the IRM and the HEM are configured so that they may be transmitted substantially simultaneously over the single twisted pair with the standard telephone signals from the phone in the guest room (206). A specific technique by which this configuration is effected is described below with reference to FIGS. 3a and 4.

Once the connection is established, the communications between the IRM and the HEM are monitored either periodically or continuously for a variety of purposes (208). This information may be used by the hotel for billing purposes or for troubleshooting and improving the reliability of the hotel network.

If an Internet transaction is requested by the guest's computer, a globally unique IP address from a pool of such addresses is temporarily associated with the network IP address currently associated with the guest's computer using, for example, a network address translation protocol (210). As discussed above, the pool of addresses could be, for example, class A, B, or C addresses. As will be discussed below with reference to FIGS. 5 and 6, the temporary association of the globally unique IP address may be done by the HEM in the hotel or, according to another embodiment, by a remote server which interconnects one or more hotel properties in a wide area network. When the Internet transaction is complete (212), the globally unique IP address is disassociated from the network IP address and put back in the pool for use in facilitating subsequent Internet transactions from any of the hotel's guest rooms (214). The network IP address remains associated with the guest's computer until the session ends, e.g., the computer is disconnected from the IRM or powered down (216).

FIGS. 3a and 3b are more detailed block diagrams of IRM 104 and HEM 124 of FIG. 1, respectively. IRM 104 comprises connection circuitry for connecting the IRM to the room's standard telephone jack as well as the room's telephone and the guest's computer. According to a specific embodiment, the connection circuitry includes RJ-11 ports 302 for connecting to the phone and 303 for connecting to the wall jack, an Ethernet port 304, an IEEE 1394 port 305, and a universal serial bus (USB) port 306 for connecting to the guest's computer, and an additional data port 307 for receiving various types of data. IEEE 1394 port 305 and USB port 306 may, in some instances, prove more convenient than Ethernet port 304 in that certain network reconfiguration issues don't have to be dealt with. In addition, many business travelers often don't travel with the Ethernet dongle which is necessary for connecting their laptop's Ethernet port to a network Ethernet port. Thus, depending upon which of the two alternate standards, IEEE 1394 or USB, the laptop is configured for, IRM 104 is operable to translate the laptop's transmissions to the Ethernet standard.

According to a specific embodiment, IRM 104 also includes transmission circuitry 308 for transmitting and receiving data on a single twisted pair of conductors of which the majority of hotel wiring infrastructures are comprised. According to one embodiment, a portion of transmission circuitry 308 is implemented according to the home PNA (Phone-line Networking Alliance) standard which allows half duplex data and phone signals on the same line as illustrated by the diagram of FIG. 4. According to the home PNA stan-

8

dard, data transmissions from IRM 104 to a port 126 of HEM 124 and transmissions from the HEM to the IRM are alternated at a frequency in the range of 4-9 MHz. Because standard phone signals exists at a relatively low frequency compared to the home PNA modulation frequency, all of the signals may easily exist on a single pair of wires.

According to a specific embodiment, transmission circuitry 308 is operable to associate the network IP address associated with IRM 104 with the guest's computer. That is, the address translation or assignment which allows the guest access to the local or wide area network is performed by the transmission circuitry in the IRM. According to a more specific embodiment, transmission circuitry 308 includes a processing unit 309 based on RISC microprocessor which performs the address translation, the combining and separation of signals for transmission to the headend, and the routing of the received signals to the appropriate IRM port. According to a specific embodiment, processing unit 309 comprises an Intel 80960VH and the appropriate support circuitry.

According to another specific embodiment, IRM 104 also includes control circuitry 310 for receiving control information via the hotel's network for controlling one or more control systems 311 proximate to the IRM. As will be discussed below with reference to FIG. 9, such control systems may include, for example, the room's temperature control, lighting, and audio systems. In one embodiment, the control circuitry includes conversion circuitry 312 for converting the received control information into the necessary control signals for actually controlling the in-room control systems. The conversion circuitry may include, for example, an RF transmission element 314 (e.g., an antenna) for transmitting RF control signals to the various control systems. According to an alternative embodiment, conversion circuitry 312 includes an infrared transmission element (e.g., an IR diode) for transmitting infrared control signals to various control systems.

Transmission circuitry 308 (using processor 309) discriminates between the various data it receives and directs it to the appropriate port on IRM 104 according to address information in data packet headers. According to a specific embodiment, digital audio and video may be transmitted to individual rooms via the system described herein. The digital audio and video are directed to additional data port 307 to which an audio and/or video system may be connected for presenting the transmitted content. In this way, an ambience may be set for the guest's arrival. In addition, the guest could select a wide variety of entertainment and information services via the hotel network which may then be transmitted to the guest's room via the auxiliary data port 307 on IRM 104. According to one embodiment, data port 307 receives audio data which directly drives a pair of speakers in the guest room.

Specific embodiments of IRM 104 also include an LED or LCD display 316 on which status and other information may be communicated to the occupant of the guest room whether or not they are currently connected. For example, before a connection is made, display 316 could be used to inform the hotel guest of all of the services available through IRM 104 as well as instructions for connecting to IRM 104. Other information such as stock quotes and weather information may also be presented continuously or periodically. Once connected, display 316 could communicate the status of the connection as well as the time connected and current connection charges. It will be understood that a wide variety of other information may be presented via display 316.

IRM 104 may also include an array of individual colored LEDs 318 which provide information to the user. Such LEDs may indicate, for example, the connection status of the IRM, i.e., whether it is connected to the HEM, using red or green

US 7,580,376 B2

9

LEDs. LEDs **318** may also be configured to indicate a purchase status to the user. That is, because connection services are often purchased in 24 hour blocks, LEDs **318** may indicate to the user whether she is operating within a block of time which has already been paid for (green), whether the end of the current block is approaching (yellow), or whether she has already entered the next time block (red). LEDs **318** could also indicate which type of connection the user has established, e.g., USB, Ethernet, or IEEE 1394.

As mentioned above and as shown in FIG. **3b**, HEM **124** may be thought of as an enhanced router which routes data packets to and from IRMs **104**, controls network access, serves as a bridge for Ethernet data transmitted over the hotel's single twisted pair infrastructure, and, according to some embodiments, handles address translation and assignment. According to one embodiment, a **2611** router from Cisco Systems, Inc. is used to implement HEM **124**. HEM **124** includes a master central processing unit (CPU) **352**, low and medium speed interfaces **354**, and high-speed interfaces **356**. When acting under the control of appropriate software or firmware, the CPU **352** is responsible for such router tasks as routing table computations and network management. It may also be responsible for controlling network access and transmissions, etc. It preferably accomplishes all these functions under the control of software including an operating system (e.g., the Internet Operating System (IOS®) of Cisco Systems, Inc.) and any appropriate applications software. CPU **352** may include one or more microprocessor chips **358**. In a specific embodiment, a memory **360** (such as non-volatile RAM and/or ROM) also forms part of CPU **352**. However, there are many different ways in which memory could be coupled to the system.

The interfaces **354** and **356** are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receipt of data packets over the network and sometimes support other peripherals used with HEM **124**. The low and medium speed interfaces **354** include a multiport communications interface **362**, a serial communications interface **364**, and a token ring interface **366**. The high-speed interfaces **356** include an FDDI interface **368** and a multiport Ethernet interface **370**. Preferably, each of these interfaces (low/medium and high-speed) includes (1) ports for communication with the appropriate media, (2) an independent processor, and in some instances (3) volatile RAM. The independent processors control such communications intensive tasks as packet switching, media control and management. By providing separate processors for the communications intensive tasks, this architecture permits the master microprocessor **352** to efficiently perform routing computations, network diagnostics, security functions, etc.

The low and medium speed interfaces **354** are coupled to the master CPU **352** through a data, control, and address bus **372**. High-speed interfaces **356** are connected to the bus **372** through a fast data, control, and address bus **374** which is in turn connected to a bus controller **376**.

Although the system shown in FIG. **3b** is one type of router by which the present invention may be implemented, it is by no means the only router architecture by which the present invention may be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc. would also be acceptable. Further, other types of interfaces and media could also be used with the router.

Regardless of network device's configuration, it may employ one or more memories or memory modules (including memory **360**) configured to store program instructions for the network operations and network access and control func-

10

tions described herein. The program instructions may specify an operating system and one or more applications, for example. Such memory or memories may also be configured to store, for example, control information for controlling in-room control systems, etc.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). The invention may also be embodied in a carrier wave travelling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Referring back to FIG. **3b**, HEM **124** has a plurality of ports **126** each of which communicates with a corresponding IRM **104**. HEM **124** has the ability to sense when any of ports **126** are being used so that the hotel may bill the user accordingly. This monitoring feature is also useful for technical support, network bandwidth requirement estimates, billing estimates, and buying pattern data. HEM **124** also has the capability of enabling and disabling individual ports **126**. Where network **100** is part of a wide area network (as discussed below), the monitoring, enabling, and disabling of ports **126** may be done from a remote server at the center of the WAN.

As described above, each HEM port **126** (and thus the corresponding IRM **104**) has a fixed IP address which may be configured using SNMP. The fixed IP address of the HEM port **126** and the IRM **104** is assigned to the guest's computer using DHCP. Alternatively, an address translation is performed between the computer's internal IP address and the fixed IP address of IRM **104**/HEM port **126**. HEM **124** has a small boot ROM **378** for basic IP communications and a large flash ROM **380** for fully functional software and configuration data. This allows for remote software upgrades using, for example, an encrypted protocol riding on top of IP.

According to various embodiments, HEM **124** also comprises transmission circuitry **316** for transmitting and receiving data on a single twisted pair of conductors. Thus, the Ethernet data which has been combined with the standard telephone signals at IRM **104** may be picked off and reconfigured for transmission according to standard Ethernet techniques. Also, data headed to IRM **104** may be combined for transmission over the single twisted pair. As with transmission circuitry **308**, transmission circuitry **316** may be implemented according to the home PNA standard.

FIG. **5** is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a chain of hotels **502** according to one embodiment of the invention. Using the internal infrastructure described above with reference to FIG. **1**, each hotel **502** has a local area network (LAN) (not shown) which provides direct access to the Internet **504** for each of its guest rooms. According to this embodiment, each hotel **502** must provide its own security in the form of a firewall **506** for the protection of its LAN.

FIG. **6** is a block diagram illustrating the provision of high speed data and Internet access to guest rooms in a chain of hotels **602** according to another embodiment of the invention.

US 7,580,376 B2

11

Using the internal infrastructure described above with reference to FIG. 1, each hotel 602 has a LAN (not shown) which is then connected with other LANs in the other hotels 602 to form a wide area network (WAN) referred to herein as a virtual private network (VPN) 604. According to a specific embodiment, VPN 604 is built on an optical fiber backbone employing asynchronous transfer mode (ATM) technology to transmit data packets. It will be understood however that any of a variety of transmission protocols and infrastructures may be employed to transmit data in such a network without departing from the scope of the present invention. Such protocols may include but are not limited to frame relay, Ethernet, and FDDI. Data are configured in the appropriate format as they leave each hotel 602 by a framer (not shown) which may be part of or associated with each hotel's router or file server.

The embodiment of FIG. 6 provides several advantages over the embodiment described above with reference to FIG. 5. High speed access to the Internet requires some form of connection to the Internet such as, for example, a T1 or T3 line. Not only does such a connection require a hardware infrastructure to support it, it also necessitates some form of protection for the network in the form of, for example, a firewall. Thus, if each hotel property in a hotel chain were to be directly connected to the Internet (as shown in FIG. 5), each property would need to have its own network hardware infrastructure, firewall, and the technical and administrative staff and functions to support the same. By contrast, with VPN 604, access to the Internet 606 is provided via a single network center (represented by remote network operation center (NOC) server 608) at which one or more firewalls 610 and any other necessary networking hardware and equipment may be located and managed. According to a specific embodiment, a redundant network center is provided in a different city than the first against the event that one or the other goes down.

Having each hotel property directly connected to the Internet is problematic for effecting control of the hotels from a central location. That is, the more each hotel LAN is amenable to control from a central location, the more vulnerable it is to hacking. With VPN 604, security is complete and centralized control is virtually unlimited. This makes things like remote software upgrades convenient thus eliminating what might otherwise be significant field service costs. In addition, because much of the equipment is centrally located, the costly redundancy of equipment and support functions at each hotel property made necessary by the embodiment of FIG. 5 is avoided.

Another important benefit of VPN 604 relates to the management of globally unique IP addresses. As mentioned above, there is a paucity of pools of globally unique IP addresses which are sufficiently large to accommodate each host on the networks of most medium to large size organizations. For example, one pool of class C addresses accommodates less than 256 simultaneous users on a network. This might be sufficient at most hotels much of the time, but it is clear that there are foreseeable circumstances where it would not be. For example, as mentioned above, if a 1200 room hotel hosted an Internet technologies seminar it is highly likely that such a pool of addresses would not be sufficient. In addition, this scenario makes the assumption that each property in a hotel chain (some comprising over 1000 properties) could procure a pool of class C addresses.

VPN 604 addresses this problem in that it spreads the IP address needs of each of the hotel properties over the resources of the entire wide area network. Thus, for example, a single class B pool of addresses might be used to accom-

12

modate all of the Internet access needs of an entire hotel chain even where the total number of rooms in the chain far exceeds the number of available globally unique IP addresses. That is, large bursts of IP address needs may occur simultaneously at dozens of the hotel properties without exhausting the nearly 64,000 globally unique addresses available in the class B pool.

Other secure services may also be provided via VPN 604. For example, video teleconferencing-over-IP 612 and voice-over-IP communications 614 may be provided to hotel guests. Moreover, by arranging access to VPN 604 by corporate hosts 616, individual employees of those corporations can have secure access to their employer's network from remote locations. Other services such as, for example, property management services 618 may be provided to the management of hotels 602.

FIG. 7 is a block diagram illustrating an auto-bauding technique which may be employed with certain alternative embodiments of the present invention. FIG. 8 is a flowchart 800 illustrating the same. Every transmission line in a hotel's wiring infrastructure has different transmission characteristics due to its length and proximity to sources of distortion. Therefore, according to a specific embodiment of the invention in which an alternative to the home PNA standard is employed, IRM 702 and HEM 704 are operable to determine the maximum data rate for each guest room individually. That is, instead of using a single rate to accommodate the slowest transmission line in the network, each room is allowed a data rate which is the maximum allowed by its transmission line. On power, IRM 702 goes to its lowest baud rate, i.e., 128 kHz (802). HEM 704 transmits empty packets at 400 microsecond intervals while IRM listens at its current baud rate (804). If communication is not established (806), an error message is generated notifying the network administrator that IRM 702 is not operational (808). If, however, communication is established (806), HEM 704 instructs IRM 702 to baud up to the next higher rate (810). If communication is established at the next higher rate (812), HEM 704 again instructs IRM 702 to baud up to the next higher rate (810). This occurs iteratively until a baud rate is reached at which communication cannot be established. At that point, IRM 702 returns to the lowest baud rate (814) and HEM 704 instructs IRM 702 to baud up to the highest baud rate at which communication was established (816). In this way, data to an from IRM 702 will always be transmitted at the maximum allowable rate.

FIG. 9 is a flowchart 900 illustrating the customization of a guest room and the transmission of control information to in-room systems via a hotel network. The ability of the present invention to provide half duplex data to each guest room over a single twisted pair connection provides additional advantages which are likely to engender further hotel customer loyalty. In recent years, the hospitality industry has been looking for customization solutions to tailor guest rooms to the needs and preferences of the individual guest. The belief is that this would go a long way toward creating the type of customer loyalty with the business traveler that airlines have created with frequent flyer programs. The basic idea is that a hotel or hotel chain keeps a database record for frequent guests in which a variety of parameters may be specified such as, for example, room temperature, lighting, background music, etc. Other customization options include various information services preferred by the guest such as, for example, stock quotes, weather reports, entertainment calendars, etc. When the guest checks in, the assigned room is then automatically configured to suit that guest's preferences.

One method of configuring the room automatically involves adjusting various controls in the room via remote

EXHIBIT 3

PAGE 66

US 7,580,376 B2

13

control signals such as, for example, radio frequency (RF) or infrared signals. According to a specific embodiment of the invention, control signals are sent to the IRM (e.g., IRM 104 of FIGS. 1 and 3a) in the guest room via the hotel network where they are converted to the appropriate form, e.g., RF, and used to set the room controls appropriately. In this way, the room's thermostat, light controls, and stereo controls may be set to provide a comfortable and familiar environment for the newly arrived guest. And, because the present invention allows half duplex data to be combined with standard telephone signals, the transmission of room control signals may be done in this manner even where the hotel wiring consists of only single twisted pair technology. In addition and as described above, digital audio and video signals as well as digital information services may be sent to the room in the same manner providing further customization capabilities. Thus, the guest room customization solution of the present invention provides a powerful tool by which individual hotels and hotel chains may engender greater customer loyalty and thereby realize increased revenues.

Referring now to FIG. 9, a specific embodiment of the invention will now be described. As described above, specific information for an individual guest is maintained in a database record 901 either on the server of a specific hotel or on a central remote server from which it may be downloaded to the specific hotel at which the corresponding guest is scheduled to arrive or is actually checking in (902). As the guest is checking in or in response to some other appropriate event, information regarding the guest's room environment and other preferences in database record 901 is transmitted from the HEM to the IRM in the guest's assigned room (904). The information is transmitted via the hotel network which may comprise the hotel's single twisted pair telephone wiring infrastructure. The in-room module then displays some of the received information, e.g., stock quotes, and converts some of the received information into an appropriate set of control signals, e.g., RF signals, for communicating with the rooms various environmental controls (906). These environmental controls may include, for example, the thermostat, lighting controls, stereo controls, television controls, etc. The appropriate adjustments are then made to the various systems in the guest room to provide the optimal environment specifically suited to the stated preferences of the arriving guest (908).

FIG. 10 is a block diagram of a file server 1000 for use with various embodiments of the present invention. File server 1000 may be used, for example, to implement any of HEM 124 of FIGS. 1 and 3a, firewall 506 of FIG. 5, and firewalls 610 and remote server 608 of FIG. 6. File server 1000 includes display 1002 and keyboard 1004, and mouse 1006. Computer system 801 further includes subsystems such as a central processor 1008, system memory 1010, fixed disk storage 1012 (e.g., hard drive), removable disk 1014 (e.g., CD-ROM drive), display adapter 1016, and network interface 1018 over which LAN, WAN, and Internet communications may be transmitted. File server 1000 operates according to network operating system software and may perform other functions such as, for example, file and database management. Other systems suitable for use with the invention may include additional or fewer subsystems. For example, another system could include more than one processor 1008 (i.e., a multi-processor system), or a cache memory (not shown).

The system bus architecture of file server 1000 is represented by arrows 1020. However, these arrows are illustrative of any interconnection scheme serving to link the subsystems. For example, a local bus could be utilized to connect the central processor to the system memory. File server 1000 is

14

but an example of a system suitable for use with the invention. Other architectures having different configurations of subsystems may also be utilized.

Various embodiments of the present invention may be used to provide special levels of service to specific groups such as, for example, the attendees of a conference at a hotel property. That is, conference attendees are identified when they connect to the hotel network and are provided access to specific content and online services which are related to the conference. FIG. 11 is a flowchart 1100 illustrating the providing of such online conference services using various ones of the network infrastructures described above such as, for example, the network environments of FIGS. 1, 3a, 3b, 5 and 6. A group identification number or tag is associated with each of the attendees of a specific conference (1102). According to a specific embodiment, this is accomplished by associating the network addresses of the IRMs in each of the guest rooms occupied by one of the attendees with the group ID tag. Conference specific services and content are then provided on the network (1104).

Conference services might include, for example, substantially real time voice communication and/or video teleconferencing with other attendees of the conference. Speakers or conference organizers may have software they want to distribute to attendees electronically. Only conference attendees have access to such electronic information. Conference specific content such as, for example, electronic copies of papers presented at the conference as well as PowerPoint® presentations are provided. Individual presenters at the conference can post follow up notes and answers to questions they were not able to get to during their presentation. Chat Rooms could be provided in which, at the end of the day, conference members can get online from their room to interact with other members. Only conference members would have access to the chat room. This service allows conference attendees to discuss questions and comments about the conference, talk about the sessions that were good and bad, critique speakers, and in general exchange information with other attendees. According to various embodiments, the chat rooms could be recorded and the information provided to conference organizers to allow them to better serve their members at future conferences. The real names of chat room participants may be excluded from this information. Bulletin boards for the posting of information by any conference attendee may also be provided. Discounted access to other services such as, for example, entertainment and information services, may also be provided.

As described above with reference to FIG. 2, when a guest's computer connects to an IRM in any one of the guest rooms, the network IP address associated with that IRM is associated with the computer (1106). As discussed above, this association could mean a DHCP assignment of the network IP address to the guest's computer where the computer did not already have an internal IP address. It could also mean that the internal IP address of the computer is translated into the network IP address. This address assignment/translation may be effected by the IRM, the HEM, or a remote server where the hotel is part of a virtual private network as described above with reference to FIG. 6.

If the network IP address associated with a particular guest's computer is associated with the group ID tag (1108), access to the conference specific services and content are provided to the user of that computer (1110). If, on the other hand, the network IP address is not associated with the group ID (1108), access to the conference specific services and content is blocked. The network IP address remains associ-

US 7,580,376 B2

15

ated with the guest's computer until the session ends, e.g., the computer is disconnected from the IRM or powered down (1114).

The technique described above with reference to FIG. 11 could be used more generally to restrict access to particular services, content, web sites, other networks, etc. to specific identifiable groups. For example, when an employee of a particular corporation checks into the hotel, the network IP address of the IRM in that employee's room may be associated with a group ID tag which will enable access to the corporation's computer (e.g., see computer host 616 of FIG. 6). As will be understood, restriction of access to a variety of content and services in this manner may be effected according to a variety of group identifications without departing from the scope of the present invention.

While the invention has been particularly shown and described with reference to specific embodiments thereof, it will be understood by those skilled in the art that changes in the form and details of the disclosed embodiments may be made without departing from the spirit or scope of the invention. For example, many of the embodiments described herein have been described with reference to hotels. It will be understood, however, that the techniques employed by the present invention may be applied to a variety of structures and institutions such as, for example, schools, office buildings, and the like. In addition, several embodiment described herein employ single twisted pair wiring which is the standard telephone wiring found in most buildings. However, it will be understood that the techniques described herein may be implemented on any of a wide variety of wiring infrastructures including, for example, Ethernet and ATM systems. Therefore, the scope of the invention should be determined with reference to the appended claims.

What is claimed is:

1. A method for restricting access to content in a network having a plurality of users associated therewith, comprising: associating a group identification tag with selected ones of the plurality of users thereby identifying the selected users as members of a specific group; providing the content on the network; and restricting access to the content to the selected users using the group identification tag by verifying that a particular network address from which a request has been received has the group identification tag associated therewith before providing access to the content.
2. The method of claim 1 wherein the specific group comprises attendees of a conference.
3. The method of claim 2 wherein the specific group comprises employees of a specific employer.
4. The method of claim 1 wherein the content relates to one or more of electronic copies of conference materials, entertainment content, online services, or web site content.
5. The method of claim 1 wherein restricting access to the content to the selected users comprises providing discounted access to entertainment content.
6. The method of claim 1 wherein restricting access to the content to the selected users comprises providing discounted access to information services.

16

7. The method of claim 1 wherein restricting access to the content to the selected users comprises providing substantially real time voice communication.

8. The method of claim 1 wherein restricting access to the content to the selected users comprises providing video teleconferencing services.

9. A method for restricting access to content in a network having a plurality of network access nodes having network addresses associated therewith each of which is unique on the network, comprising:

associating the network addresses with computers associated with a plurality of users while the computers are connected to the network access nodes thereby providing access to the network for each of the plurality of users;

associating a group identification tag with the network address associated with selected ones of the plurality of users thereby identifying the selected users as members of a specific group;

providing the content on the network; and restricting access to the content to the selected users using the group identification tag.

10. The method of claim 9 wherein selected ones of the computers have internal IP addresses and associating the network addresses with the selected computers comprises translating the internal IP addresses to the network addresses.

11. The method of claim 9 wherein selected ones of the computers do not have internal IP addresses and associating the network addresses with the selected computers comprises assigning the network addresses to the computers.

12. The method of claim 9 wherein the network comprises a local area network and associating the network addresses is done by a headend associated with the local area network.

13. The method of claim 9 wherein the network comprises a wide area network and associating the network addresses is done by a remote server which controls the wide area network.

14. The method of claim 9 wherein associating the network addresses is done by the network access nodes.

15. A network configured to restrict access to content in the network, the network comprising:

a plurality of network access nodes having network addresses associated therewith each of which is unique on the network; and

at least one computing device programmed to:

associate the network addresses with computers associated with a plurality of users while the computers are connected to the network access nodes thereby providing access to the network for each of the plurality of users;

associate a group identification tag with the network address associated with selected ones of the plurality of users thereby identifying the selected users as members of a specific group;

provide the content on the network; and restrict access to the content to the selected users using the group identification tag.

* * * * *